



УКРАЇНА

(19) UA (11) 89651 (13) C2  
(51) МПК (2009)  
H04L 9/14

МІНІСТЕРСТВО ОСВІТИ  
І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ  
ІНТЕЛЕКТУАЛЬНОЇ  
ВЛАСНОСТІ

## ОПИС ДО ПАТЕНТУ НА ВІНАХІД

### (54) СПОСІБ ШИФРУВАННЯ ДВІЙКОВИХ БЛОКІВ ДАНИХ (ВАРІАНТИ)

1

(21) а200705535

(22) 21.05.2007

(24) 25.02.2010

(46) 25.02.2010, Бюл.№ 4, 2010 р.

(72) ГОРБЕНКО ІВАН ДМИТРИЙОВИЧ, ДОЛГОВ  
ВІКТОР ІВАНОВИЧ, ОЛІЙНИКОВ РОМАН ВАСИ-  
ЛЬОВИЧ, ЛИСИЦЬКА ІРИНА ВІКТОРІВНА(73) ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИ-  
ТЕТ РАДІОЕЛЕКТРОНІКИ

(56) RU 2206961 C2; 20.06.2003

UA 53949 A; 17.02.2003

RU 2249857 C2; 10.04.2005

RU 2212108 C2; 10.09.2003

GB 2123589 A; 01.02.1984

FR 2627036 A1; 11.08.1989

EP 0454505 A2; 30.10.1991

US 5321689 A; 14.06.1994

(57) 1. Спосіб шифрування двійкових блоків даних, який складається з виконання за допомогою набору підключів, сформованих з майстер-ключа, ітеративної процедури криптографічних перетворень, яка включає первинне забілювання вихідного блока за допомогою додавання у суматорі за модулем 2 з першим підключем, і наступних циклових перетворень, кожне з яких включає подання вхідного блока двійкових даних у вигляді послідовності байтів, його додавання у блоці складання із черговим підключем, також представленим у вигляді послідовності байтів, здійснення заміни кожного байта отриманої побайтової суми новим байтом відповідно до таблиці підстановки, а після проходження всіх циклів зашифрування виконання післяциклового ключового перетворення шляхом додавання у відповідному пристрої із останнім підключем, який **відрізняється** тим, що на вході ітеративної процедури криптографічних перетворень вводять додатне циклове перетворення, яке включає на першому етапі підсумування вхідного блока даних у суматорі за модулем два із цикловим підключем, розбивку двійкового блока даних після підсумування на два напівблоки, що представляють байтовими рядками, наступне виконання першого шару керованих підстановок, який в свою чергу включає послідовну заміну кожного байта кожного напівблока новим байтом відповідно до таблиці підстановки, причому байтовий вхід підстановки формують шляхом додавання за допомогою суматора за модулем два поточного бай-

2

та кожного напівблока до байта на виході блока заміни цього ж напівблока, отриманого на попередньому кроці, причому для першого байта кожного напівблока даних додавання виконується зі значенням останнього байта даного напівблока, що дозволяє після виконання операцій підстановок сформувати два нових байтових напівблоки, а на другому етапі - повторне підсумування отриманих байтових напівблоків у суматорах за модулем два із додатними цикловими підключами, взаємне перемішування отриманих після підсумування байтових напівблоків шляхом подання їх двома байтовими напівблоками, кожний з яких складається з парних байтів одного напівблока й непарних байтів іншого напівблока, наступного виконання другого шару байтових керованих підстановок для байтів кожного з цих напівблоків, узятих у зворотному порядку проходження, причому для першого у зворотному порядку байта кожного напівблока даних як керуючий використовують байт, що є сумою за модулем два всіх байтів вихідного блока даних, отриманих після його підсумування із цикловим підключем, подальшого об'єднання байтових виходів підстановок у блок даних на виході циклової функції, причому використовуване число циклів і відповідно розмірність простору вироблюваних підключів для вихідної ітеративної процедури криптографічних перетворень беруть зменшеним до двох разів.

2. Спосіб шифрування двійкових блоків даних, який складається з виконання за допомогою набору підключів, сформованих з майстер-ключа, ітеративної процедури криптографічних перетворень, яка включає первинне забілювання вихідного блока за допомогою підсумування вхідного блока даних у суматорі за модулем два з першим підключем, наступних циклових перетворень, кожне з яких включає подання вхідного блока двійкових даних у вигляді послідовності байтів, їх підсумування у проміжному суматорі за модулем два із черговим підключем, також представленим у вигляді послідовності байтів, здійснення заміни кожного байта отриманої побайтової суми новим байтом відповідно до таблиці підстановки, й наприкінці заключне перетворення за допомогою підсумування у вихідному суматорі за модулем два блока даних, отриманого після циклових перетворень, із останнім підключем, при цьому в про-

(13) C2

(11) 89651

(19) UA

цедурі розгортання ключів використовується циклове перетворення основної процедури шифрування, який **відрізняється** тим, що в циклових перетвореннях використовують керовані підстановки із взаємним управлінням по входах, де на першому етапі здійснюють розбивку двійкового блока даних після підсумування із цикловим підключем на два напівблоки, що представляють байтовими рядками, наступне виконання першого шару байтових керованих підстановок, який включає заміну кожного байта напівблока новим байтом відповідно до таблиці підстановки, причому байтовий вхід підстановки формують шляхом додавання за модулем два поточного байта напівблока до байта на виході блока заміни, отриманого на попередньому кроці, причому для першого байта кожного напівблока даних додавання виконується зі значенням останнього байта даного напівблока, що дозволяє після виконання операції першого шару керованих підстановок сформувати два нових байтових напівблоки, а на другому етапі - повторне підсумування отриманих байтових напів-

локів у суматорах за модулем два із додатними цикловими підключами, взаємне перемежування отриманих після підсумування байтових напівблоків шляхом подання їх двома байтовими напівблоками, один з яких складається з парних байтів одного напівблока, а другий з непарних байтів іншого напівблока, наступного виконання другого шару байтових керованих підстановок для байтів кожного з цих напівблоків, узятих у зворотному порядку проходження, причому для першого у зворотному порядку байта кожного напівблока даних як керуючий використовують байт, що є сумою за модулем два всіх байтів вихідного блока даних, отриманих після його підсумування із цикловим підключем, подальшого об'єднання байтових виходів підстановок у блок даних на виході циклової функції, причому використовуване число циклів беруть зменшеним до трьох разів, а в процедурі розгортання майстер-ключа циклове перетворення теж заміняють перетворенням з керованими підстановками.

Винахід відноситься до області обчислювальної техніки, а саме до способів криптографічного перетворення даних.

Відомий спосіб недетермінованого криптографічного перетворення даних [патент UA №53949, МПК 7 H04L29/14, Публ. Бюл. №2, кн.1, 2003]. Спосіб включає формування ключа шифрування у вигляді сукупності підключів і почергове перетворення підблоків на основі керованої підстановки (байтовій заміні), при котрому таблицю підстановок представляють у вигляді латинського прямокутника, розмірність якого визначається підблоком, що підлягає зашифруванню а саме перетворення здійснюють на основі керованої підстановки, шляхом вибору як вихідний байт значення осередку таблиці, обумовленої по першому (інформаційному) входу в таблицю підстановок по рядках (стовпцях), значенням підблоку що шифрується на поточному кроці, і другому (керуючому) входу в таблицю по стовпцях (рядках), обумовленому байтовим значенням виходу таблиці підстановок на попередньому кроці, по черзі у двох напрямках, причому в одному напрямку використовують підстановки-рядки, в іншому - підстановки-стовпці латинського прямокутника, а між перетвореннями в кожному з напрямків вводять операцію додавання підблоків даних із ключем, що вибирають параметрично залежним від значення останнього зашифрованого підблоку попередньої поточної операції керованої підстановки.

Недоліком цього способу є недостатня захищеність шифру від атак диференційного та лінійного криптоаналізу (можливе побудування диференційних та лінійних характеристик з малим числом активних S-блоків). Крім того, потрібний значний обсяг пам'яті для зберігання таблиці підстановок великого розміру, що обмежує використання шифру в ряді практичних додатків.

Найбільш близьким по сукупності істотних ознак до способу, що заявляється, є спосіб, реалізований у шифрі AES Rijndael [див. V. Rijmen.

«AES Proposal: Rijndael», AES Round 1, National Institute of Standards and Technology, Aug 1998. <http://www.nist.gov/aes/>], що складається в здійсненні багатоциклової процедури криптографічних перетворень, яка виконується за допомогою набору підключів, що включає первинне забілювання вихідного блоку даних за допомогою додавання за модулем два (XOR) з першим підключем і наступні ітеративні циклові перетворення, котрі в свою чергу використовують набір перетворень позначених відповідно AddRoundKey() - перетворення в якому циклічний підключ складається з масивом State (проміжним результатом шифрування блоку даних), ShiftRows() - перетворення, яке обробляє масив State шляхом циклічного зсуву останніх трьох його рядків на різні значення зсувів, SubBytes() - перетворення, що діє на вхідний масив State за допомогою нелінійної таблиці байтової підстановки, яка незалежно діє на кожному байті масиву State, а також набір операцій: XOR (виключне АБО), множення багаточленів за модулем  $x^4+1$  й множення в скінченному полі. Специфічні функції (перетворення) використовують й у процедурі розгортання ключів: RotWord() (функція, що перетворює слово з чотирьох байтів в нове слово й виконує над ним циклічну перестановку. SubBytes() (функція бере вхідне слово з чотирьох байтів й застосовує перестановку (S-блок) до кожного із чотирьох байтів для одержання вихідного слова. При розгортанні ключів також використовують масив циклічних констант Rcon[]].

Хоча даний спосіб характеризується досить високою швидкістю процедури зашифрування-розшифрування, однак за сучасними мірками продовжує відчуватися необхідність подальшого нарощування продуктивності алгоритмів симетричного шифрування. У наведеному способі основне обмеження по швидкодії процедури зашифрування-розшифрування, пов'язане з використанням у цикловій функції операції множення на матрицю (при зашифруванні) і зворотної операції ділення

(при розшифруванні), а також з використанням досить великого (більше 14) числа циклів ітеративної процедури криптографічних перетворень. Крім того, як впливає з публікацій, у процесі досліджень стійкості алгоритму Rijndarl для нього був виявлений ряд потенційних слабкостей, які, щоправда, сьогодні не можна вважати скільки-небудь небезпечними, але з ними в перспективі, можливо, необхідно буде порахуватися.

Технічною задачею винаходу є створення способу криптографічного перетворення двійкових даних, що має більш високі показники стійкості й швидкодії.

Ця технічна задача вирішується тим, що в способі шифрування двійкових блоків даних, що складається з виконання за допомогою набору підключів, сформованих з майстра-ключа, ітеративної процедури криптографічних перетворень, яка включає первинне забілювання вихідного блоку за допомогою додавання за модулем 2 з першим підключом і наступних циклових перетворень, кожне з яких включає подання вхідного блоку двійкових даних у вигляді послідовності байтів, його додаванні із черговим підключом також представленим у вигляді послідовності байтів, здійснені заміни кожного байта отриманої побайтової суми новим байтом відповідно до таблиці підстановки (блоку підстановки), а після проходження всіх циклів зашифрування виконані після циклового ключового перетворення у вигляді додавання з останнім підключом, відповідно винаходу перше циклове перетворення замінюють новим, яке включає на першому етапі розбивку двійкового блоку даних після сумування із цикловим підключом на два напівблоки, що представляють байтовими рядками, наступну заміну кожного байта напівблоку новим байтом відповідно до фіксованої таблиці підстановки (блоку табличної заміни), причому байтовий вхід підстановки формують шляхом додавання за модулем два поточного байта напівблоку до байту на виході блоку заміни, отриманому на попередньому кроці (для першого байта кожного напівблоку даних додавання виконується зі значенням останнього байта даного напівблоку), що дозволяє після виконання операції підстановки (першого шару керованих підстановок) сформувати два нових байтових напівблоки, а на другому етапі - сумування нових байтових напівблоків за модулем два (XOR) з двома цикловими підключами, кожний з котрих є циклічним зсувом додатного циклового підключа на число бітів, що задають значенням семи бітів останнього байта кожного напівблоку першого шару підстановок, причому останні байти додатних циклових підключів замінюють нульовими значеннями, подальшого взаємного перемищення (перестановки) отриманих після сумування із додатними цикловими підключами байтових напівблоків шляхом подання їх двома байтовими напівблоками (рядками), кожний з яких складається з парних байтів одного напівблоку й непарних байтів іншого напівблоку, наступного повторного виконання процедури байтових керованих підстановок (другого шару керованих підстановок) для байтів кожного з рядків цих напівблоків, узятих у зворотному порядку проходження, причому для першого

(в зворотному порядку) байта кожного напівблоку даних як керуючий використовують байт що є сумою за модулем два всіх байтів вихідного блоку даних після сумування із цикловим підключом, подальшого об'єднання байтових виходів підстановок (конкатенації вихідних напівблоків, сформованих у результаті виконання операцій заміни байтів для кожного із нових напівблоків), у блок даних на виході циклової функції, причому використовуване число циклів і відповідно розмірність простору вироблюваних підключів (з точністю до одного додатного циклового підключа) беруть зменшенням до двох разів.

Нова сукупність істотних ознак дозволяє реалізувати початкове циклове перетворення, що має поліпшені властивості щодо перемішування та розсіювання, а також підвищену стійкість до відомих кріптоатак й за рахунок цього скоротити число циклів шифрування, тобто підвищити швидкодію без зниження (або з поліпшеними залежно від числа відкинутих циклів) показників криптографічної стійкості.

Нижче сутність запропонованого рішення більш докладно викладається з посиланнями на приведені фігури.

На Фіг.1 представлена структура одного циклу нового перетворення.

На Фіг.2 представлена схема одного кроку байтової заміни (керованої підстановки).

На Фіг.3 представлена блок-схема пристрою, що реалізує нове циклове перетворення.

Фіг.4 ілюструє результати тестування шифру Rijndarl за допомогою комплексу, що складається з 146 тестів

Фіг.5 ілюструє результати тестування X9.17 Gost 64, за допомогою комплексу, що складається з 146 тестів

Фіг.6 ілюструє результати тестування шифру з керованими підстановками (4-х циклове перетворення), за допомогою комплексу, що складається з 146 тестів

Фіг.7. ілюструє результати тестування генератора Rijndarl, за допомогою комплексу NIST STS.

Фіг.8. ілюструє результати тестування генератора X9.17 Gost 64, за допомогою комплексу NIST STS.

Фіг.9. ілюструє результати тестування генератора на ЕК, за допомогою комплексу NIST STS.

Фіг.10. ілюструє результати тестування шифру з керованими підстановками (4-й циклове перетворення), за допомогою комплексу NIST STS.

Табл.1. Показники лавинного ефекту для шифру, побудованого на основі циклових перетворень із керованими підстановками, для довжини блоку даних 256 бітів і такої ж довжини майстра-ключа.

У відповідності із структурою нового циклового перетворення (Фіг.1), вхідний блок даних 1 після додавання з цикловим підключом 2 розбивається на два напівблоки, які інтерпретуються байтовими рядками 3, 4. Після цього байти кожного рядка 3 і 4 подаються послідовно на входи керованих підстановок - блоки заміни 5 і 6 (один для кожного рядка напівблоків), які виконують операції керованої підстановки відповідно до Фіг.2.

Як впливає з Фіг.2, на вхід кожного блоку підстановки разом з кожним черговим байтом рядка подається шляхом додавання з ним за модулем два результати байтової заміни попереднього кроку, тобто значення байта на виході блоку заміни на попередньому кроці є керуючим для блоку заміни на поточному кроці (на вхід перших блоків заміни для кожного напівблоку як керуюче подається значення останнього байта напівблоку). У підсумку байтів рядок кожного з напівблоків перетворюється після проходження блоку заміни в новий байтів рядок.

Далі для отриманих на виходах блоків заміни двох байтових напівблоків 7, 8 (Фіг.1) виконують операцію сумування за модулем два (XOR) з додатними цикловими підключами у блоках 9 та 10. Остаточне значення циклових підключів визначається для кожного напівблоку значеннями останніх (16-го для 128 бітного напівблоку) байтів на виходах першого шару керуючих підстановок (байтове значення в потрібний діапазон вводиться шляхом відкидання одного з бітів), і на основі отриманого значення виконується циклічний зсув кожного циклового підключу на відповідну кількість бітів, при цьому останні байти сформованих підключів замінюються нульовими.

Далі виконується взаємне перемищення (перестановки) результуючих байтових напівблоків, шляхом подання їх двома новими байтовими напівблоками (рядками) 11, 12, кожний з яких складається з парних байтів одного напівблоку й непарних байтів іншого напівблоку, подальшого повторного виконання процедури байтових керування підстановок 13, 14 для байтів кожного з рядків нових напівблоків, узятих у зворотному порядку проходження, причому для першого байта кожного напівблоку даних додавання виконують із байтом, що є сумою за модулем два всіх байтів блоку даних після сумування із цикловим підключем, далі виконується об'єднання байтових виходів підстановок (конкатенації вихідних напівблоків, сформованих у результаті виконання операцій заміни байтів для кожного із нових напівблоків) у блок даних 15 на виході циклової функції.

Подальша пропозиція, сформульована у варіанті 2 формули винаходу, використовує переваги запропонованого циклового перетворення для побудування цілковитого нового шифру, де на всіх циклах застосовується процедура керованої підстановки, при цьому виключається найбільш часозатратна операція циклової функції прототипу - додаткове (після підстановки) лінійне перетворення.

До переваг запропонованого циклового перетворення можна віднести те, що зміна будь-якого біта вхідного блоку даних навіть можливі зміни всіх наступних за зміненним підблоків, а за рахунок подвійного проходу, коли перед другим проходом здійснюється перестановка напівбайтів, забезпечується поліпшена збалансованість участі кожного байта у формуванні результату зашифрування. У підсумку практично вже за один такий цикл досягається максимально можлива чутливість результату перетворення до зміни кожного біта вхідного блоку даних і ключа (запропонована підстановочно-перестановочна операція найбільш повно реа-

лізує ідею Шеннона по ефективному розсіюванню й перемішуванню). Ця принципова властивість дозволяє перейти до зменшеного в порівнянні із прототипом числу циклів перетворення й цим істотно підвищити загальну швидкість процедури шифрування в цілому. Можливі резерви подальшого підвищення швидкодії полягають також у тому, що запропонована процедура допускає одночасне виконання операцій перетворення для окремих напівблоків.

Зупинимось більш детально на оцінці стійкості запропонованих рішень по побудуванню процедури шифрування до відомих методів криптоаналізу.

Обґрунтування стійкості запропонованого способу шифрування при зменшеному в порівнянні із прототипом числом циклових перетворень. Представляється принциповим для обґрунтування ефективності запропонованого способу довести, що нове одноциклове перетворення забезпечує запас такої стійкості відносно найбільш важливих типів атак - лінійного та диференційного криптоаналізу (при зменшеному в порівнянні з прототипом загальному числі циклів криптографічних перетворень), котрий гарантує можливість зменшення загального числа циклів перетворень, тобто потрібно показати, що один цикл нового перетворення забезпечує стійкість супротив відмічених атак не меншу ніж стійкість, яку забезпечується половиною циклових перетворень прототипу. Нижче ми зупинимось на обґрунтування цього факту, та наведемо додатні міркування стосовно підвищених показників стійкості запропонованого способу у відношенні інших відомих атак.

Стійкість до лінійного й диференційного криптоаналізу. Відносно підвищеної стійкості до відомих методів криптоаналізу, і, зокрема, до лінійного й диференційного криптоаналізу можна відзначити, що за рахунок використання механізму керованої підстановки реально варто очікувати відсутності будь-яких статистично стійких асиметричних (змішених по ймовірності) зв'язків між входами й виходами циклових перетворень і всього шифру в цілому.

Додатково можна привести наступні міркування. Як впливає з публікацій [див., наприклад, Р. Junod and S. Vandenay. Fox: a new family of block ciphers. To appear in Selected Areas in Cryptography 2004: Waterloo, Canada, August 9-14, 2004], можна побудувати S-блоки з байтовими переходами значень диференційних ймовірностей переходів

$DP_{max}^{Sbox}$ , й ймовірностей лінійних апроксимацій

$LP_{max}^{Sbox}$  на нелінійність, й цьому забезпечити алгебраїчну нелінійність що дорівнює 6. Ймовірність результуючої диференційної характеристики ви-

значається формулами  $\left( DP_{max}^{Sbox} \right)^r$ ,  $\left( LP_{max}^{Sbox} \right)^r$

або  $\left( DP_{max}^{Sbox} \right)^{2r}$ ,  $\left( LP_{max}^{Sbox} \right)^{2r}$  (в залежності від

кількості шарів блоків заміни). Для розглянутого рішення результат циклового перетворення за рахунок використання керованих підстановок буде змінюватися непередбаченим образом, тому що різниця в текстах в одному байті буде викликати

ненульові різниці на виходах усіх наступних S-блоків (ненульова різниця на виході даного S-блоку буде формувати ненульові керуючі входи у всі наступні підстановки), тобто будуть активуватись усі (або майже всі) наступні S-блоки. Це означає, що ймовірність одноциклового переходу буде вже дорівнювати не менш ніж  $(2^{-4})^{32} = 2^{-128}$  (ми вже не кажемо про те, що потрібно ще "зшити" характеристики на різних циклах перетворень, тобто необхідно буде ще домогтися того, щоб характеристика S-блоку чергового циклу була погоджена з характеристикою попереднього). А це означає, що вже при 4 циклах криптографічних перетворень варто очікувати, що ймовірність результуючої диференційної характеристики як і ймовірність результуючої лінійної апроксимаційної характеристики вже буде оцінюватися значенням  $(2^{-128})^4 = 2^{-512}$ .

При більш докладному аналізі можна ще розглядати ситуацію ненульових входів (різниць) для двох сусідніх S-блоків одного шару підстановок, причому припустити, що різниця чергового S-блоку нівелює (збігається з байтом різниці керуючого входу) ненульову різницю, що приходить із керуючого входу. Тоді всі наступні S-блоки першого шару підстановок при відповідних умовах не будуть активізуватися (відносно проходженню різностей). В розглянутому рішенні таке нівелювання можна зробити у граничному випадку для двох перших S-блоків першого шару підстановок. Але за рахунок того, що для першого S-блоку другого шару підстановок в якості керуючого використовується байт, що є сумою за модулем два усіх байтів вхідного блоку даних (після сумування з цикловим підключенням), ненульове значення різниці входів для S-блоків першого шару підстановок буде давати ненульове значення різниці на керуючому вході першого S-блоку другого шару підстановок, котре буде розповсюджуватись на всі інші S-блоки другого шару підстановок. Отже, будуть активізуватися усі S-блоки другого шару підстановок. В результаті для випадку активізації одного S-блоку першого шару підстановок та 32 S-блоків другого шару підстановок, з урахуванням того, що в цьому випадку при обчисленні ймовірності диференційної характеристики циклового перетворення до ймовірності переходу різностей одного (першого) S-блоку

$DP_{\max}^{Sbox}$  при проході одного шару підстановок потрібно буде внести додатковий коефіцієнт, який при прийнятті гіпотези про рівномірний розподіл значень різниць окремих байтів для різних блоків (напівблоків) даних може бути оціненим як  $2^{-8} = 1/256$  (тут 256 - число варіантів входів в S-блок), у граничному випадку, що розглядається, для ймовірності одноциклового переходу можна розглядати значення  $2^{-8}(2^{-4})(2^{-4})^{32} = 2^{-142}$ . Але це ще не все. Для отримання цього результату потрібно буде ще зшити характеристики переходів для S-блоків обох шарів підстановок, що представляється дуже малоймовірним. Нарешті, при обчисленні диференційних характеристик наступних циклів треба враховувати активними підстановки обох шарів, що приводить до оцінки для ймовірності одноциклової диференційної характеристики (без урахування умов зшивки характеристик окремих S-блоків)

$$\left( DP_{\max}^{Sbox} \right)^{64} = \left( 2^{-4} \right)^{64} = 2^{-256}, \text{ що забезпечує}$$

потрібні характеристики стійкості вже за один цикл наступного перетворення.

Відмічений принцип активізації підстановок другого шару, однак, може бути порушеним, якщо за рахунок активізації останнього (16-го при 128 бітному напівбайті) S-блоку першого шару підстановок здійснити нівелювання (занулення) результату (різниць) при проході першого S-блоку другого шару підстановок, на керуючий вхід котрого відповідно до запропонованого способу буде підведене байтове значення  $x_1 \oplus x_2 \oplus x_{16} \oplus S_{\llcorner 1} \oplus x_{16} \rceil$  (розглядується випадок, коли активізується перший S-блок, на керуючий вхід котрого підводиться значення останнього байта напівблоку  $x_{16}$ , так що на його виході формується значення  $S_{\llcorner 1} \oplus x_{16} \rceil$ , й при цьому вхідне значення другого байта напівблоку даних нівелює попередній результат, отриманий при проході першого S-блоку, тобто  $x_2 = S_{\llcorner 1} \oplus x_{16} \rceil$ . Отже виходить, що коли

$S_{\llcorner 16} \rceil = x_1 \oplus x_2 \oplus x_{16} \oplus S_{\llcorner 1} \oplus x_{16} \rceil$ , то на виході першого напівблоку другого шару підстановок буде формуватись нульове байтове значення і тому наступні підстановки активізуватись не будуть (усі S-блоки другого шару підстановок мають вхідне нульове значення виходів першого шару підстановок окрім останнього S-блоку другого шару підстановок, входом для котрого буде ненульове значення різниці на виході першого S-блоку першого шару підстановок). В результаті очікуваного лавинного розповсюдження активізації на S-блоки другого шару підстановок здійснюватися не буде. Для захисту від цієї слабкості в схему введений "сторож", задача котрого перекрити ситуації, коли значення байта на виході останнього S-блоку першого шару підстановок (на вході першого S-блоку другого шару підстановок можна підібрати таким, щоб воно збіглося би із байтовим значенням керуючого входу. Для цього служить динамічна зміна значень введених додатно циклових підключів, яка здійснюється на основі використання значень виходів останніх підстановок першого шару. В цій ситуації коли буде здійснюватися спроба виконати атаку диференційного криптоаналізу на циклову функцію, нападаючому для отримання нульового значення різниці на виході першої підстановки другого шару підстановок необхідно буде вибрати відповідні різні значення виходів останньої підстановки першого шару підстановок, але тоді для цих різних значень відповідно до способу будуть формуватись різні циклові підключи, котрі будуть приводити до активізації майже всіх S-блоків другого шару підстановок (вихідні різниці майже всіх підстановок першого шару нульові). Отже, виходить, що запропоноване одноциклове перетворення буде забезпечувати стійкість супротив атак диференційного криптоаналізу не більш високу ніж можна отримати за сім циклових перетворень прототипу.

Враховуючи дуальний зв'язок, що існує між диференційним та лінійним криптоаналізом, слід очікувати повну захищеність запропонованого спо-

собу шифрування й від атак лінійного криптоаналізу.

Інтегральна атака. Інтегральна атака застосовується до шифрів з добре вибудованою структурою, подібної SPN структурі. Тому що запропонована циклова функція відрізняється від звичайно застосовуваної в SPN конструкції наявністю недетермінованого механізму (за рахунок використання підстановок, керованих поточними станами процедури криптографічного перетворення), то представляється, що навряд чи вдасться знайти інтегральний розрізнявач для цілої структури всього шифру.

Інші атаки.

Статистичні атаки. З огляду на високі дифузійні властивості циклової функції, високий степінь нелінійності S блокового перетворення навіть для малого числа циклів можна із упевненістю казати, що запропоновані рішення будуть стійкими до всіх варіантів лінійного й диференційного криптоаналізу і їхніх сполучень, до бумерангових і rectangle атак та їхніх узагальнень, подібним до атак з використанням усічених диференціалів і диференціалів високого порядку, неможливих диференціалів і багатьох інших атак.

Відносно-ключова й слайд атаки. Слайд атаки експлуатують періодичну структуру алгоритму розгортання ключів. Завдяки дуже гарній дифузії й високій нелінійності запропонованої в п.2 нової процедури розгортання підключів, представляється досить мало ймовірним, що відносно-ключові й слайд атаки будуть ефективними для запропонованого рішення.

Інтерполяційні й алгебраїчні атаки. Інтерполяційні атаки використовують переваги S-блокового подання, а саме просту алгебраїчну структуру S-блоку. Якщо використати S-блоки, наприклад, запропоновані авторами шифру FOX, то це нелінійне відображення не піддається простому опису над  $GF(2)$  або  $GF(2^8)$ . Більше того, сам недетермінований механізм, реалізований за допомогою керованих підстановок, навряд чи може знайти аналітичний опис (на наш погляд вимоги до відбору підстановок у запропонованому рішенні можуть виявитися істотно більше м'якими, ніж, наприклад, у шифрі FOX). Тому представляється, що відзначені атаки не є скільки-небудь ефективними для запропонованих рішень.

Запропоноване нове одноциклове перетворення може бути реалізовано за допомогою пристроїв, представлених разом із з'єднаннями між ними блок-схемою на Фіг.3, де блок 1 - суматор за модулем два (XOR), блок 2 - накопичувач циклового підключа, блоки 3, 4 - накопичувачі напівблоків даних (байтових рядків) після сумування з цикловим підключем, 5, 6 - блоки керованих підстановок першого шару перетворень, блоки 7, 8 - накопичувачі байтових рядків (напівблоків) з виходів керованих підстановок, 9, 10 - блоки сумування напівблоків з додатними цикловими підключами, 11, 12 - блоки перемешення, 13, 14 - блоки керованих підстановок другого шару перетворень, блок 15 - накопичувач вхідного блоку даних, блок 16 - накопичувач додатного циклового підключа, 17, 18 - регістри-накопичувачі циклічних зсувів циклового підключа (з зануленням останніх байтів), 19 - бага-

товхідний суматор за модулем два (XOR) байтових значень блоку даних, отриманного після сумування вхідного блоку даних з цикловим підключем на вході циклової функції.

Байтовий рядок (блок вхідних даних) подається на перший вхід блоку 1 (суматора), до другого входу якого підключений вихід регістра-накопичувача циклового підключа 2, вихід суматора підключений до входів блоків 3 та 4, у свою чергу підключених своїми виходами до входів блоків 5 і 6, а виходи блоків 5 і 6 відповідно до входів блоків 7 і 8. Ці блоки свою чергу підключених своїми виходами до входів блоків 9, 10. Виходи останніх підключені відповідно до входів блоків 11, 12, причому до кожного з цих блоків на керуючий вхід подається байт з виходу блоку 19 (ці входи позначені пунктиром, тому що задіяні лише для перших S блоків кожного шару підстановок), який формується шляхом сумування за модулем два байтів з виходів блоку 1. Байтові виходи блоків 11 і 12 підключені своїми виходами до входів блоків 13, 14, виходи котрих поєднуються в загальний блок перетворених даних, що вводиться в накопичувач 15. Блок даних на виході накопичувача 15 є виходом циклової функції. Для формування додатних циклових підключів кожного з напівблоків загальний ключ зчитується з накопичувача 16, з виходу котрого два напівблоки подаються на регістри-накопичувачі циклічного зсуву 17, 18, керуючі входи котрих підключені до виходів відповідних керуючих підстановок першого шару.

Реалізація запропонованого способу не викликає утруднень, тому що всі блоки й вузли, що входять у пристрій, що реалізує спосіб, загальновідомі й широко описані в технічній літературі.

Далі наведені деякі результати експериментальної оцінки показників статистичної безпеки запропонованої процедури, а також прототипу й деяких інших шифруючих перетворень.

У табл.1 представлені результати аналізу лавинного ефекту, реалізованого в експериментах із шифром, побудованим на керованих підстановках. Приводяться числа одиничних і нульових елементів у побітовій різниці зашифрованих блоків на виході кожного циклу для пар блоків даних на вході шифру, що відрізняються одним бітом.

З таблиці 1 видно, що у всіх випадках змінюється половина біт зашифрованого тексту з відхиленням 0.003%. Видно також, що відхилення відбувається в обидва боки, і, отже, при збільшенні кількості випробувань відхилення повинне зменшитися ще більше. Виконавши відповідні експерименти при збільшенні числа випробувань до 1000000, приходимо до відхилення, що перебуває в діапазоні значень 0.001%. Отримані результати свідчать, що показники лавинного ефекту (глибина входу в цикли шифру й дисперсія відхилень від середнього значення) краще всіх відомих криптографічних алгоритмів, у тому числі й прототипу. Результати оцінки лавинного ефекту при зміні одного (кожного) біта ключа показують, що картина залишається тієї ж самою.

Для більш глибокої оцінки показників статистичної безпеки, були виконані дослідження статистичних характеристик запропонованої конструкції шифру з керованими підстановками в режимі ге-

нерації гами шифруючої, тобто шифр використався для генерування псевдовипадкової послідовності. Існує два комплекси тестування статистичних характеристик послідовностей. Один з них розроблений сторонньою фізичною особою, інший розроблений національним інститутом стандартів США «NIST STS (Statistical Test Suite)». На Фіг.4-6 наведені підсумкові результати тестування запропонованого алгоритму й відомих алгоритмів за допомогою першого комплексу, що складає з 146 тестів.

Порівняльний аналіз отриманих результатів показує, що Rijndarl посів перше місце, алгоритм, заснований на циклах з керованими підстановками (4 цикли) посів друге місце, а X9.17 Gost 64 посів третє місце.

Результати тестування цих же шифрів, а також шифру на еліптичних кривих (ЭК) комплексом NIST STS, що складається з 189 тестів представлені на Фіг.7-10.

Кількість тестів для шифру Rijndarl, у яких тестування пройшло 99% послідовностей дорівнює 145. Кількість тестів, у яких тестування пройшло більше 96% послідовностей дорівнює 189.

Кількість тестів для генератора X9.17 Gost 64, у яких тестування пройшло 99% послідовностей, дорівнює 139. Кількість тестів, у яких тестування пройшло більше 96% послідовностей, дорівнює 187.

Кількість тестів для генератора на ЭК, у яких тестування пройшло 99% послідовностей, дорівнює 146. Кількість тестів, у яких тестування пройшло більше 96% послідовностей, у цьому випадку дорівнює 188.

Кількість тестів для генератора на керованих підстановках (4 цикли), у яких тестування пройшло 99% послідовностей, дорівнює 131. Кількість тестів, у яких тестування пройшло більше 96% послідовностей, дорівнює 186.

Отримані результати свідчать, що генератор, заснований на циклах з керованими підстановками, по показниках статистичної безпеки перебуває приблизно на одному рівні з генераторами, побудованими на відомих шифрах. Більше точна оцінка, показує, що (для чотирьохциклової конструкції шифру з керованими підстановками) три тести не пройшли 96% рівень, що вважається рекомендованим граничним значенням. Збільшення числа циклів до 8 привело до того, що вже тільки два тести не пройшли 96% граничний рівень. Очевидно, що при подальшому збільшенні кількості циклів можна домогтися необхідних статистичних показників, хоча більше кращої є подальша модернізація запропонованого алгоритму.

Слід зазначити, що вище наведені результати експериментів відносяться до циклової функції в вигляді двох шарів підстановок без ділення вхідного блоку даних на два напівблоку. Для випадку використання запропонованої у формулі винаходу конструкції вже за один цикл такого перетворення (навіть без введення циклового підключення) вдається забезпечити проходження усіх тестів.

Таким чином, підводячи підсумки обговоренню й обґрунтуванню можливостей реалізації (досяг-

нення) заявлених переваг запропонованих технічних рішень, можна відзначити наступні положення.

Стійкість криптографічних перетворень базується на завданні ключової невизначеності, у той час як алгоритм перетворень є відомим (правило Керкхоффа). Ця обставина відкриває значні можливості для успішного проведення криптоаналізу багатьох існуючих криптографічних схем. Очевидно, що логічна невизначеність, впроваджена в шифр у подібних випадках, значно утрудняє проведення багатьох атак.

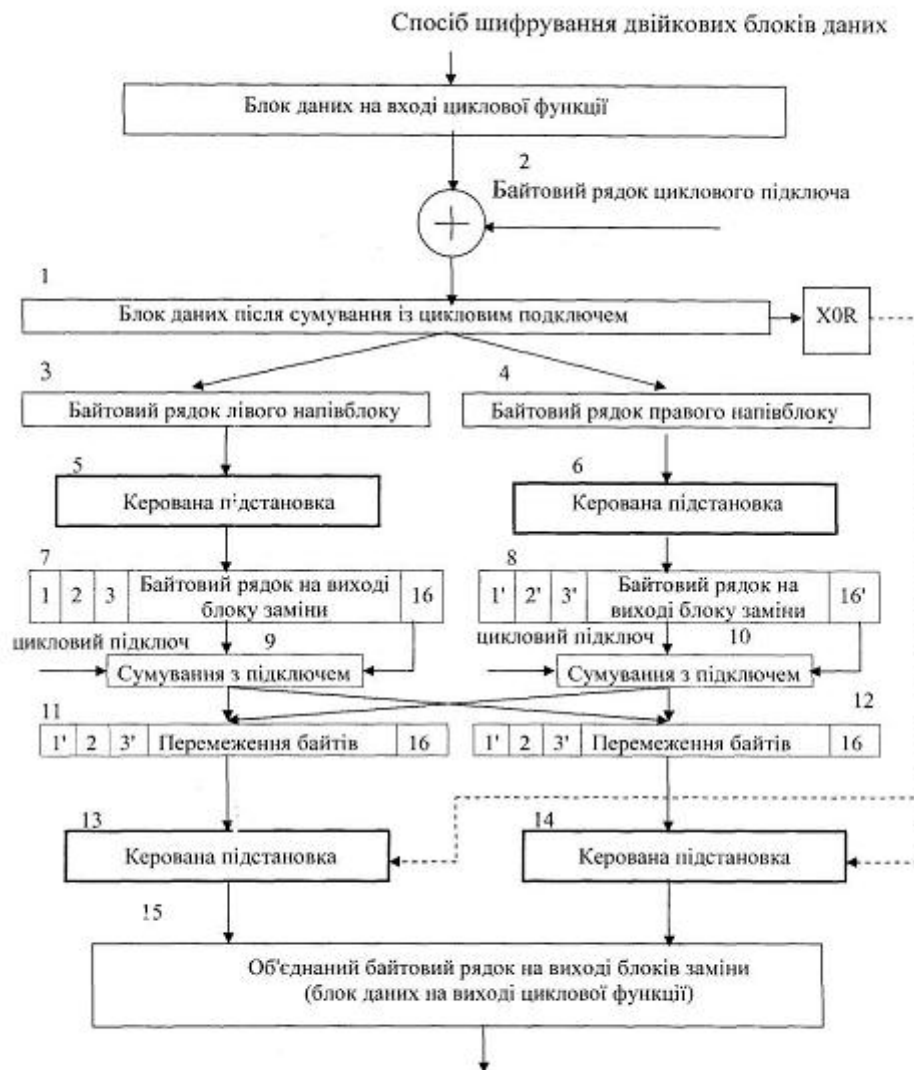
Аналіз існуючих криптографічних перетворень із метою побудови ключезалежного способу шифрування показує, що з лінійних перетворень, найбільш кращою є операція «XOR». Вона володіє рядом переваг у порівнянні з іншими, такими як швидкість виконання операції, високий степінь волі результату, що забезпечує досягнення гарних показників декореляції перетворених значень. Інша проста розповсюджена операція - параметричний зсув володіє рядом недоліків, які обмежують її застосування при побудові високозахисних криптографічних систем. До основних недоліків тут можна віднести невисокий степінь свободи результату, нестабільні кореляційні показники. Так у випадку, коли певний блок складається зі значних наборів нулів або одиниць або має ідентичні частини, операція параметричного зсуву не змінює вихідного значення на багатьох позиціях (табличне подання операції циклічного зсуву показує, що підстановки які її описують, не суперечливі, що свідчить про нестабільні кореляційні показники операції). Застосування операції випадкової перестановки також представляється не завжди виправданим, внаслідок значної безлічі слабких (не суперечливих) підстановок. Очевидно, що перевагу в багатьох випадках варто віддати суперечливим підстановкам і близьких до них, що володіють кращими показниками розсіювання. Цей тип нелінійної операції одержав велике поширення й успішно застосовується в таких шифрах як NOEKEON, Rijndael, DES, Гост 28147 і т.д. Недоліком використання однієї і тієї ж підстановки можна вважати необхідність додаткового захисту від частотного аналізу. У випадку, коли блок складається з однакових підблоків, після виконання підстановки, перемішування блоку не відбувається. Перераховані недоліки зникають при використанні різних підстановок. Аналіз й експерименти свідчать, що застосування керованої підстановки є в багатьох випадках істотно більш кращим. Кількість підстановок використовуваних шифром повинна забезпечувати високий степінь волі результату, що сприяє гарному розсіюванню. Поряд з відомими реченнями по використанню великих матриць суперечливих підстановок розміром 256x256, у запропонованому рішенні обґрунтовується можливість застосування для реалізації процедури керованої підстановки таблиць підстановок істотно менших розмірів.

Результати аналізу існуючих перетворень у цілому показують, що використання недетермінованих процедур криптографічних перетворень й, зокрема, процедур керованих підстановок, дозволяє уникнути багатьох слабкостей фіксованих детермінованих перетворень.

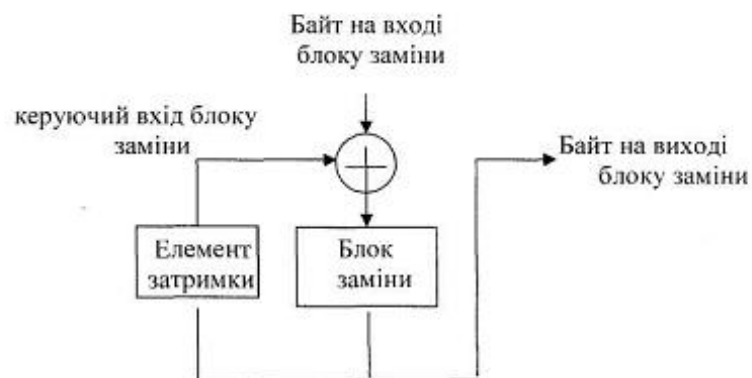
Таблица 1

Цикл	Маска		
	1000000000000000	0100000000000000	0010000000000000
1	640604 > 639524 - 1080	640317 > 639811 - 506	640753 > 639375 - 1378
2	640506 > 639622 - 884	639740 < 640388 - 648	639627 < 640501 - 874
3	639753 < 640375 - 622	640044 < 640084 - 40	639967 < 640161 - 194
4	639508 < 640620 - 1112	640461 > 639667 - 794	640004 < 640124 - 120
5	639613 < 640515 - 902	640328 > 639800 - 528	640500 > 639628 - 872
6	639863 < 640265 - 402	640075 > 640053 - 22	640623 > 639505 - 1118
7	640514 > 639614 - 900	640705 > 639423 - 1282	639856 < 640272 - 416
8	639965 < 640163 - 198	639050 < 641078 - 2028	640560 > 639568 - 992
9	639713 < 640415 - 702	640390 > 639738 - 652	640339 > 639789 - 550
10	640075 > 640053 - 22	641093 > 639035 - 2058	640964 > 639164 - 1800
11	640198 > 639930 - 268	639980 < 640148 - 168	639896 < 640232 - 336
12	640529 > 639599 - 930	640353 > 639775 - 578	639642 < 640486 - 844
13	640714 > 639414 - 1300	640102 > 640026 - 76	640391 > 639737 - 654
14	639963 < 640165 - 202	640872 > 639256 - 1616	641149 > 638979 - 2170
15	640050 < 640078 - 28	639355 < 640773 - 1418	640290 > 639838 - 452
Цикл	0001000000000000	0000100000000000	0000010000000000
1	639716 < 640412 - 696	639902 < 640226 - 324	640064 < 640064 - 0
2	639650 < 640478 - 828	63974K 640387 - 646	639723 < 640405 - 682
3	640941 > 639187 - 1754	640964 > 639164 - 1800	640372 > 639756 - 616
4	640877 > 639251 - 1626	640330 > 639798 - 532	639870 < 640258 - 388
5	640321 > 639807 - 514	641219 > 638909 - 2310	640621 > 639507 - 1114
6	640463 > 639665 - 798	641047 > 639081 - 1966	640594 > 639534 - 1060
7	640424 > 639704 - 720	639900 < 640228 - 328	639918 < 640210 - 292
8	640369 > 639759 - 610	640160 > 639968 - 192	639843 < 640285 - 442
9	640012 < 640116 - 104	639697 < 640431 - 734	640053 < 640075 - 22
10	639829 < 640299 - 470	640225 > 639903 - 322	640053 < 640075 - 22
11	639169 < 640959 - 1790	39762 < 640366 - 604	640172 > 639956 - 216
12	640496 > 639632 - 864	639890 < 640238 - 348	639674 < 640454 - 780
13	639780 < 640348 - 568	640305 > 639823 - 482	640505 > 639623 - 882
14	640306 > 639822 - 484	640454 > 639674 - 780	640206 > 639922 - 284
15	639828 < 640300 - 472	640133 > 639995 - 138	640526 > 639602 - 924

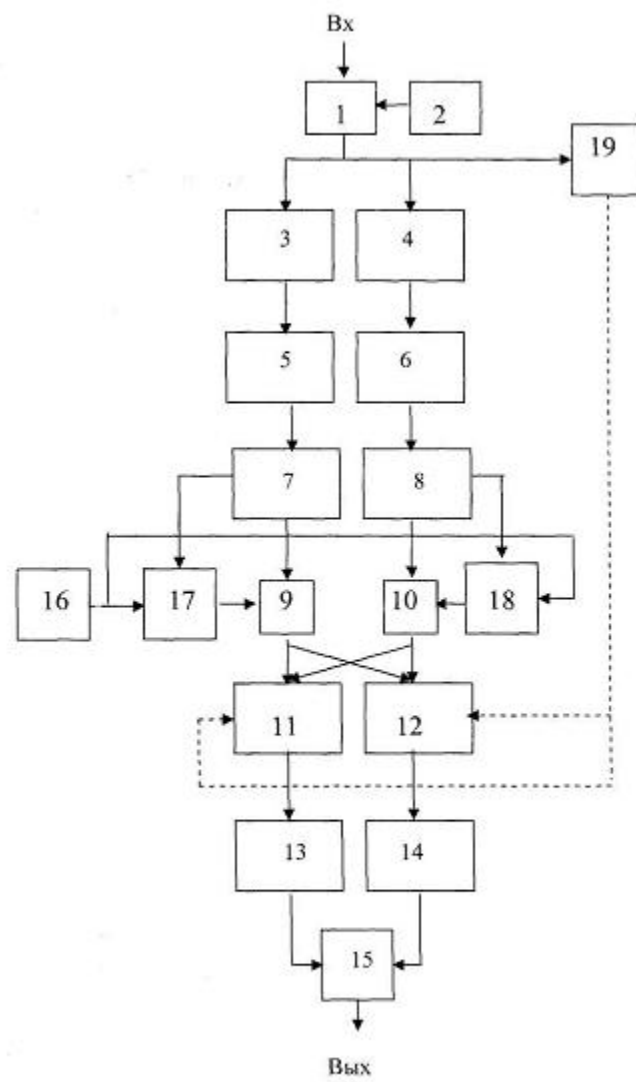




Фіг. 1



Фіг. 2



Фиг. 3



Фиг. 4

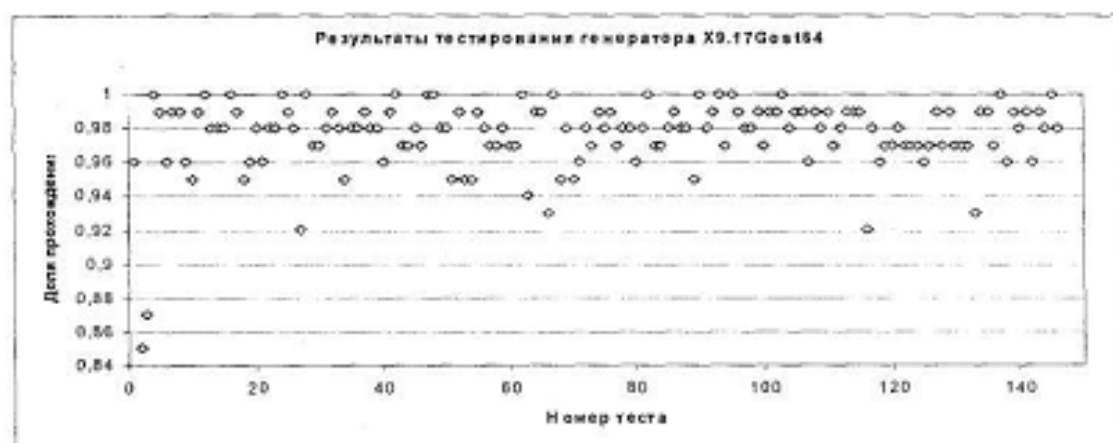


Fig. 5

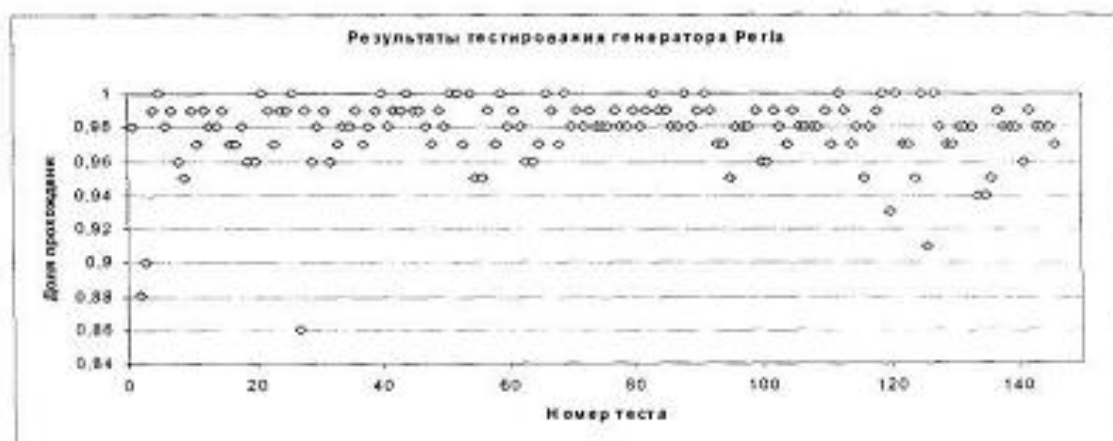


Fig. 6

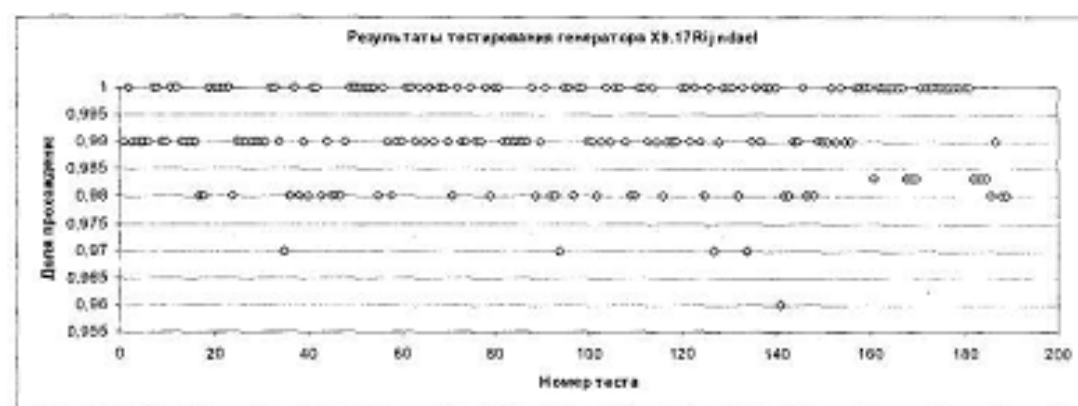


Fig. 7

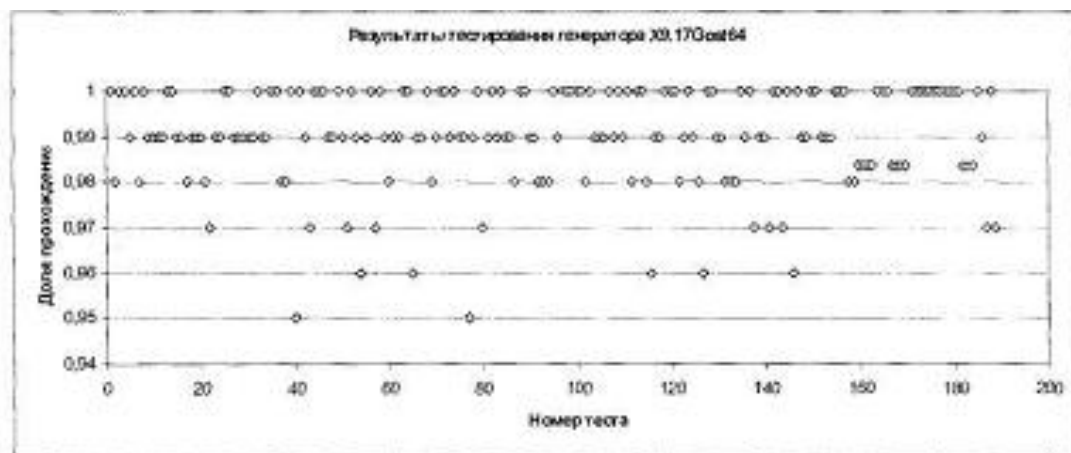


Fig. 8

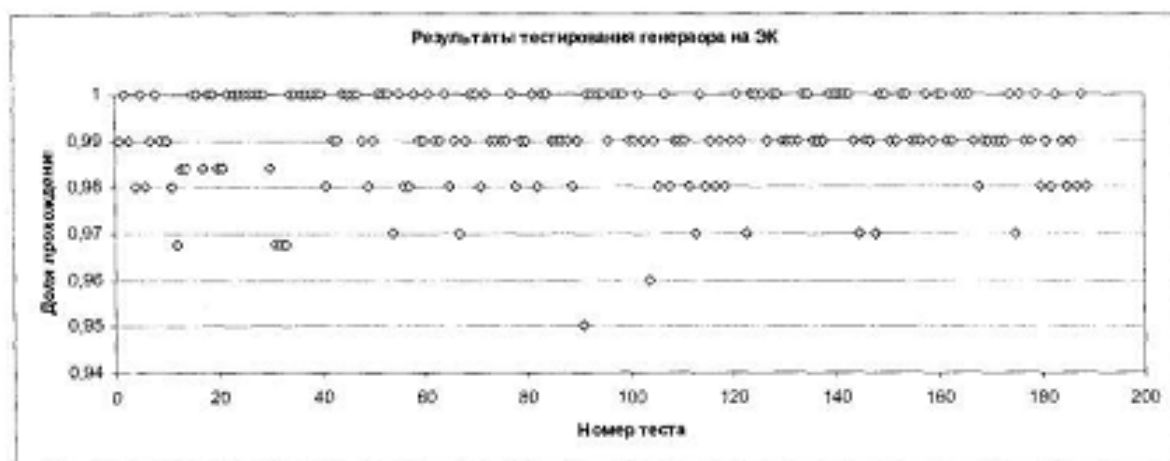


Fig. 9



Fig. 10

