



УКРАЇНА

(19) UA

(11) 156501

(13) U

(51) МПК

G06F 17/10 (2006.01)

НАЦІОНАЛЬНИЙ ОРГАН
ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ
ДЕРЖАВНА ОРГАНІЗАЦІЯ
"УКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ
ОФІС ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ ТА ІННОВАЦІЙ"

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2023 05558**

(22) Дата подання заявки: **20.11.2023**

(24) Дата, з якої є чинними
права інтелектуальної
власності: **04.07.2024**

(46) Публікація відомостей
про державну
реєстрацію: **03.07.2024, Бюл.№ 27**

(72) Винахідник(и):

**Николайчук Ярослав Миколайович (UA),
Сегін Андрій Ігорович (UA),
Возна Наталя Ярославівна (UA),
Грига Володимир Михайлович (UA)**

(73) Володілець (володільці):

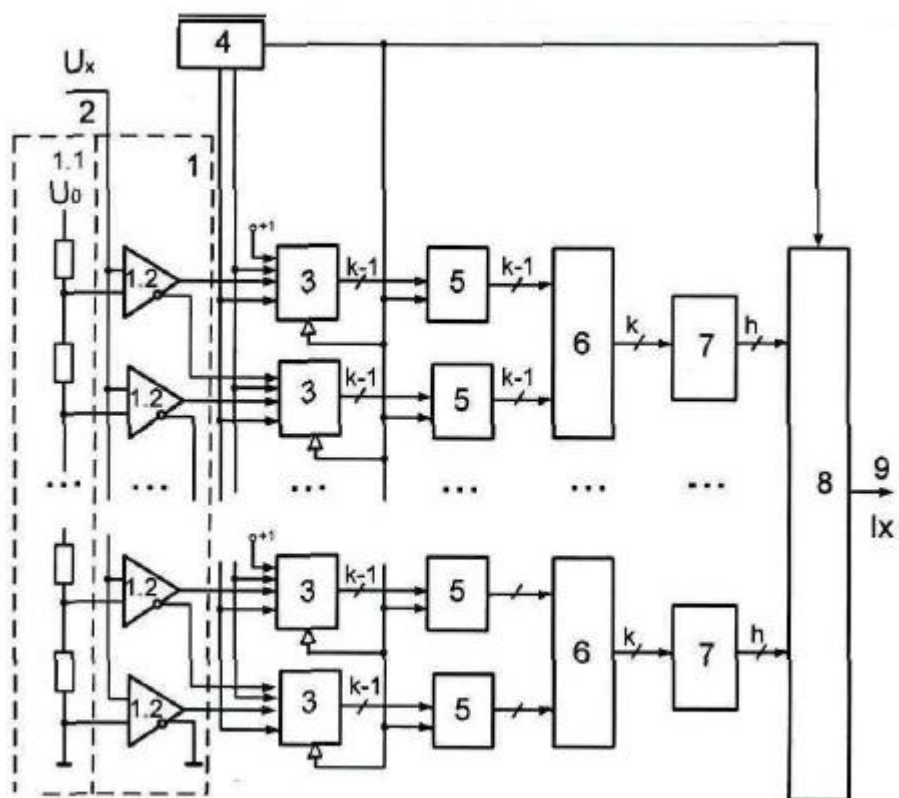
Николайчук Ярослав Миколайович,
вул. В. Великого, 14-а, м. Надвірна, Івано-
Франківська обл., 78400 (UA),
Сегін Андрій Ігорович,
вул. С. Бандери, 70, кв. 26, м. Тернопіль,
Тернопільська обл., 46011 (UA),
Возна Наталя Ярославівна,
вул. Київська, 11-б, кв. 21, м. Тернопіль,
Тернопільська обл., 46016 (UA),
Грига Володимир Михайлович,
пров. І. Богуна, 12, м. Надвірна, Івано-
Франківська обл., 78400 (UA)

(54) ПРИСТРІЙ ДЛЯ ВИЗНАЧЕННЯ ЕНТРОПІЇ

(57) Реферат:

Пристрій для визначення ентропії містить аналого-цифровий перетворювач (АЦП), вхід якого з'єднаний з входом пристрою, синхронізатор, лічильники, шифратори та пірамідальний суматор. Вхід АЦП з'єднаний з першими входами всіх парафазних компараторів. Другі входи яких з'єднані з відповідними виходами взірцевих резисторів. Другий вихід синхронізатора з'єднаний з другим входом пірамідального суматора та другими входами всіх лічильників. Перші входи пірамідального суматора з'єднані з виходами відповідних шифраторів, а його вихід є виходом пристрою, в якому перший вихід синхронізатора з'єднаний з першими входами всіх лічильників. Прямий вихід i -го компаратора у кожному каналі з'єднаний з третім входом i -го лічильника. Інверсний вихід $(i+1)$ -го компаратора з'єднаний з четвертим входом i -го лічильника, виходи якого з'єднані з відповідними першими входами i -го регістра пам'яті. Другий вхід всіх регістрів пам'яті з'єднаний з другим виходом синхронізатора. У кожному i -му каналі пристрою додатково введено два $(k-1)$ -розрядні двійкові лічильники, jk -входи яких, відповідно, з'єднані з прямими виходами i -тих компараторів та інверсними виходами $(i+1)$ -тих компараторів. Виходи, відповідно, з'єднані з входами додатково введених 1-го та 2-го $(k-1)$ -розрядних регістрів пам'яті, виходи яких додатково з'єднані з відповідними входами додатково введеного k -розрядного двійкового суматора, виходи якого додатково з'єднані з входами i -го шифратора, а входи синхронізації других $(k-1)$ -розрядних лічильників з'єднані між собою та додатково введеним третім виходом синхронізатора.

UA 156501 U



Фиг. 2

Пристрій належить до засобів обчислювальної техніки і може бути використаний для розрахунку ентропії випадкових процесів шляхом визначення ймовірнісної міри ентропії за оцінкою К. Шеннона при побудові спецпроцесорів систем передавання криптозахищених даних та приймачів ентропійно-маніпульованих сигналів.

Відомий аналог [1] - пристрій для визначення ентропії, який містить аналого-цифровий перетворювач (АЦП), вхід якого з'єднаний з входом пристрою, синхронізатор, логічні елементи, лічильники, шифратори та пірамідальний суматор, у кожному каналі містить лічильник, вихід якого з'єднаний з входом шифратора, вихід якого з'єднаний з відповідним першим входом пірамідального суматора, вихід якого є виходом пристрою, в якому вхід АЦП з'єднаний з першими входами всіх парафазних компараторів, другі входи яких з'єднані з відповідними виходами взірцевих резисторів, прямий вихід кожного i -го компаратора з'єднаний з першим входом i -го логічного елемента І-НІ, другий вхід якого з'єднаний з другим інверсним виходом $(i+1)$ -го компаратора, третій вхід всіх логічних елементів І-НІ з'єднаний з першим виходом синхронізатора, другий вихід якого з'єднаний з другим входом пірамідального суматора і першим входом всіх лічильників, другі входи яких з'єднані з виходами відповідних логічних елементів І-НІ.

Недоліком такого пристрою є низька швидкодія, яка обумовлена тим, що процеси накопичення p_i у лічильниках кожного каналу пристрою, перетворення кодів у шифраторах та додавання вихідних добутоків $p_i \log_2 p_i$ у пірамідальному суматорі здійснюється в одному циклі роботи пристрою з сумарною затримкою сигналів в одному мікроциклі.

Найближчим аналогом до корисної моделі є пристрій для визначення ентропії [2, фіг. 1], який містить аналого-цифровий перетворювач АЦП, вхід якого з'єднаний з входом пристрою, синхронізатор, лічильники, шифратори та пірамідальний суматор, при цьому вхід АЦП з'єднаний з першими входами всіх парафазних компараторів, другі входи яких з'єднані з відповідними виходами взірцевих резисторів, другий вихід синхронізатора з'єднаний з другим входом пірамідального суматора та другими входами всіх лічильників, перші входи пірамідального суматора з'єднані з виходами відповідних шифраторів, а його вихід є виходом пристрою, в якому перший вихід синхронізатора з'єднаний з першими входами всіх лічильників, прямий вихід кожного i -го компаратора з'єднаний з третім входом i -го лічильника, інверсний вихід $(i+1)$ -го компаратора з'єднаний з четвертим входом i -го лічильника, виходи якого з'єднані з відповідними першими входами i -го регістра пам'яті, виходи якого з'єднані з відповідними входами i -тих шифраторів, а другий вхід всіх регістрів пам'яті з'єднаний з другим виходом синхронізатора.

Недоліком такого пристрою є низька швидкодія, яка обумовлена тим, що процес накопичення суми ймовірностей p_i , у кожному каналі пристрою здійснюється із затримкою сигналів 2 мікротакти у компараторах та 2 мікротакти у JK-тригерах. Наприклад, при об'ємі вибірки ($n=256$) вихідних кодів АЦП, загальна затримка сигналів у одному каналі пристрою складає $4n=1024$ (мікротакти).

В основу корисної моделі поставлена задача підвищення швидкодії пристрою для визначення ентропії шляхом додаткового введення у кожному i -му каналі пристрою двох $(k-1)$ -розрядних двійкових лічильників, двох $(k-1)$ -розрядних регістрів пам'яті та k -розрядного комбінаційного двійкового суматора, що дозволяє здійснювати обчислення суми $(p_{j1}+p_{j2})$ у кожному i -му розряді пристрою паралельно двома $(k-1)$ -розрядними лічильниками із зсувом сигналів їх синхронізації на 1 мікротакт, що дозволяє підвищити швидкодію накопичення суми p_i у 2 рази швидше у порівнянні з відомим аналогом.

Поставлена задача вирішується тим, що пристрій для визначення ентропії, який містить аналого-цифровий перетворювач (АЦП), вхід якого з'єднаний з входом пристрою, синхронізатор, лічильники, шифратори та пірамідальний суматор, при цьому вхід АЦП з'єднаний з першими входами всіх парафазних компараторів, другі входи яких з'єднані з відповідними виходами взірцевих резисторів, другий вихід синхронізатора з'єднаний з другим входом пірамідального суматора та другими входами всіх лічильників, перші входи пірамідального суматора з'єднані з виходами відповідних шифраторів, а його вихід є виходом пристрою, в якому перший вихід синхронізатора з'єднаний з першими входами всіх лічильників, прямий вихід i -го компаратора у кожному каналі з'єднаний з третім входом i -го лічильника, інверсний вихід $(i+1)$ -го компаратора з'єднаний з четвертим входом i -го лічильника, виходи якого з'єднані з відповідними першими входами i -го регістра пам'яті, другий вхід всіх регістрів пам'яті з'єднаний з другим виходом синхронізатора, згідно з корисною моделлю, у кожному i -му каналі пристрою додатково введено, два $(k-1)$ -розрядні двійкові лічильники, jk -входи яких, відповідно, з'єднані з прямими виходами i -тих компараторів та інверсними виходами $(i+1)$ -тих компараторів, а виходи, відповідно, з'єднані з входами додатково введених 1-го та 2-го $(k-1)$ -розрядних

регістрів пам'яті, виходи яких додатково з'єднані з відповідними входами додатково введеного k-розрядного двійкового суматора, виходи якого додатково з'єднані з входами i-го шифратора, а входи синхронізації других (k-1)-розрядних лічильників з'єднані між собою та додатково введеним третім виходом синхронізатора.

В основу роботи пристрою покладено застосування парафазних компараторів, швидкодія яких перевищує типову швидкодію JK-тригерів на один порядок, введення у кожному каналі двох (k-1)-розрядних регістрів пам'яті та k-розрядного двійкового суматора, а також зміщеної у часі на 1 мікротакт тактової синхронізації двійкових лічильників дозволило підвищити швидкодію роботи пристрою у 3 рази.

При цьому додаткова затримка сигналів внаслідок додаткового введення у кожному каналі пристрою k-розрядних суматорів не впливає на загальну швидкодію удосконаленого пристрою, оскільки сумарна затримка сигналів після реєстрації даних, у регістрах пам'яті набагато менша, у порівнянні із затримкою сигналів у накопичуючих лічильниках кожного каналу і складає:

$\tau = (2+1+2+4+11 \times 5+8 \times 6+2)+8=114+8=122 < 307$, де 114 - затримка сигналів паралельного процесу обчислень у відомому пристрої, 8 - додаткова затримка сигналів додатково введеного k-розрядного суматора, 307 - затримка сигналів у накопичуючих лічильниках удосконаленого пристрою.

Суть корисної моделі пояснюють креслення, на яких зображено: на фіг. 2 показано структурну схему пристрою, який містить: 1 - АЦП, 2 - інформаційний вхід пристрою, 1.1 - група взірцевих резисторів, 1.2 - компаратори з парафазними виходами (прямим та інверсним), 3 - лічильники, 4 - синхронізатор, 5 - регістри пам'яті, 6 - суматори; 7 - шифратори, 8 - пірамідальний суматор, 9 - вихід пристрою. Як компоненти суматори 6 та пірамідальний суматор 8 застосований однорозрядний двійковий суматор з прямими входами та виходами (Фіг. 3).

Пристрій працює наступним чином. На початку кожного циклу визначення ентропії сигналом другого виходу синхронізатора (4) всі лічильники (3) скидаються у нульовий стан, одночасно їх вихідні коди записуються у відповідні регістри пам'яті (5), а з виходу суматора (9) зчитується код визначеної ентропії попереднього циклу обчислень. Сигнали першого та третього виходу синхронізатора (4) із зміщенням сигналів синхронізації на 1 мікротакт на інтервалі вибірки об'єму випадкових подій 2^k тактують роботу лічильників (3).

На інтервалі циклу роботи пристрою у кожному (k-1)-розрядному лічильнику 3 накопичується відповідне число імпульсів p_i та p_j , коди яких подаються на відповідні входи регістрів пам'яті (5), вихідні коди яких, у кожному каналі додаються у k-розрядному суматорі (6) та таблично формуються у шифраторах (7) коди добутоків $(p_i+p_j) \times \log_2(p_i+p_j)$, які надходять на відповідні перші входи багаторозрядного пірамідального суматора (8). У кожному циклі роботи пристрою сигналами 2-го та 3-го виходів синхронізатора (4), які подаються на перші входи лічильників (3), здійснюється накопичення їх сум.

Формування імпульсів p_i та p_j на входах лічильників (3) здійснюється шляхом з'єднання виходів (i+1)-тих та i-тих компараторів з відповідними J- та K-входами синхронних лічильників (3), структурна схема яких разом зі з'єднаними регістрами пам'яті (5) зображена на Фіг. 4.

Записані у (k-1)-розрядних регістрах пам'яті, значення (p_i+p_j) додаються у k-розрядному двійковому суматорі, паралельно з новим циклом накопичення сум ймовірностей у кожному каналі, згідно виразу:

$$\tau = \begin{cases} \tau_{ПК} + \tau_T / 2; \\ \tau_T + \tau_{\Sigma 1} + \tau_{\Sigma} + \tau_{\Sigma 2} \end{cases},$$

де $\tau_{ПК}=0,2$, швидкодія застосованого парафазного компаратора, перевищує типову швидкодію переключення JK-тригера у 10 разів, згідно з сучасними мікротехнологіями (Фіг. 5, Фіг. 6) [4, рис. 30, $f=318$ MHz], [3, таблиця переключення JK-тригера, $f_{ТР}=35$ MHz]; $\tau_T=2$; $\tau_{\Sigma}=\log_2 k$; $\tau_{\Sigma}=4$; $\tau_{\Sigma 2}=h \times \tau + k \times \tau_S$, при $n=256$, $k=8$, $h=11$; $\tau_+=(1 \div 5)$; $\tau_S=(1 \div 6)$ [2].

Таким чином затримка сигналів в n-циклах роботи пристрою визначається згідно з виразом:

Тобто, затримка сигналів, у відомому пристрої, в одному циклі накопичення суми ймовірностей p_i складає: $\tau_1=256 \times (2+2)=1024$ (мікротакти). Відповідно в удосконаленому пристрої затримка сигналів накопичення ймовірностей складає: $\tau_2=256 \times (0,2+1)=307$.

Загальна затримка сигналів у паралельному циклі обчислень запропонованого пристрою $\tau=(2+8+4+11 \times 5+11 \times 6)+8=135+8=143$ (мікротакти), що не впливає на загальну швидкодію пристрою.

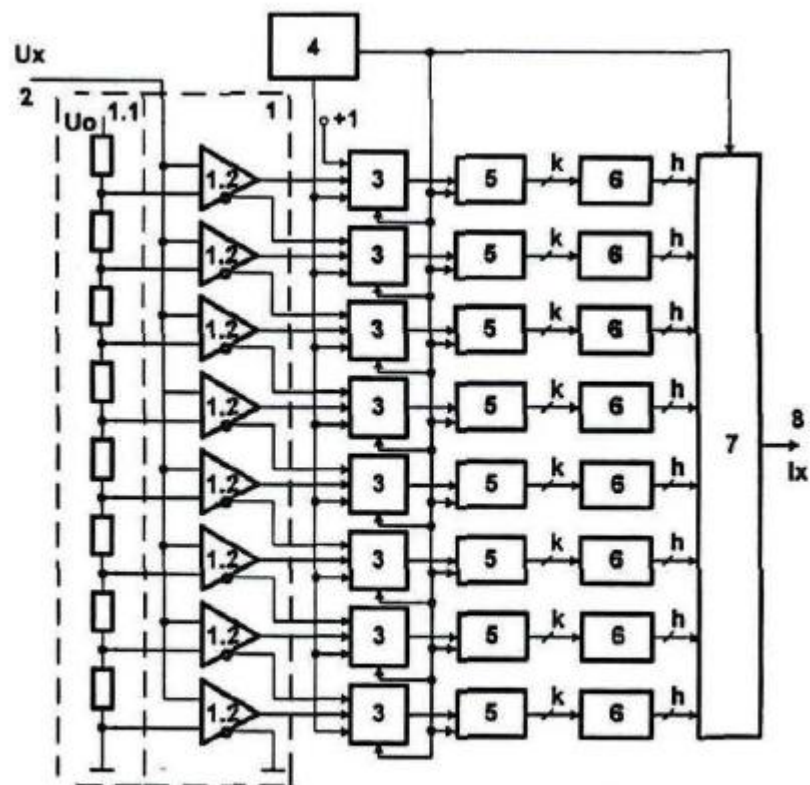
Таким чином, у порівнянні з відомим аналогом підвищення швидкодії запропонованого пристрою, відповідно становить $1024/307=3,4$ рази.

Список використаних джерел

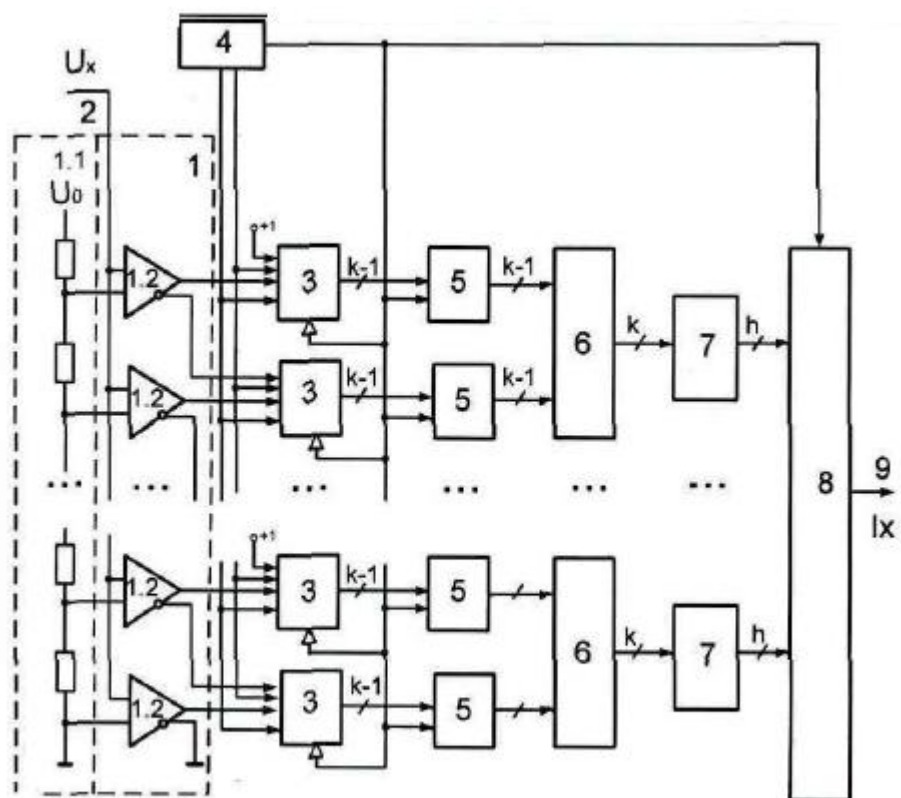
1. Воронин А.Р., Николайчук Л.М., Возна Н.Я., Пастух Т.І. Пристрій для визначення ентропії. Патент на корисну модель № 121046 (бюл. № 22 від 27.11.2017 р.)
2. Пастух Т.І., Николайчук Л.М., Возна Н.Я., Воронич А.Р., Сегін А.І. Пристрій для визначення ентропії. Патент на винахід № 123920 (бюл. № 25 від 23.06.2021р.)
3. <http://www.ti.com/lit/ds/svmlink/lmh7324> (рис. 30)
4. <https://studvlib.net/doc/18470539/7470-dual-positive-edge-triggered-i-k-flip-flop> (таблиця характеристики переключення)

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

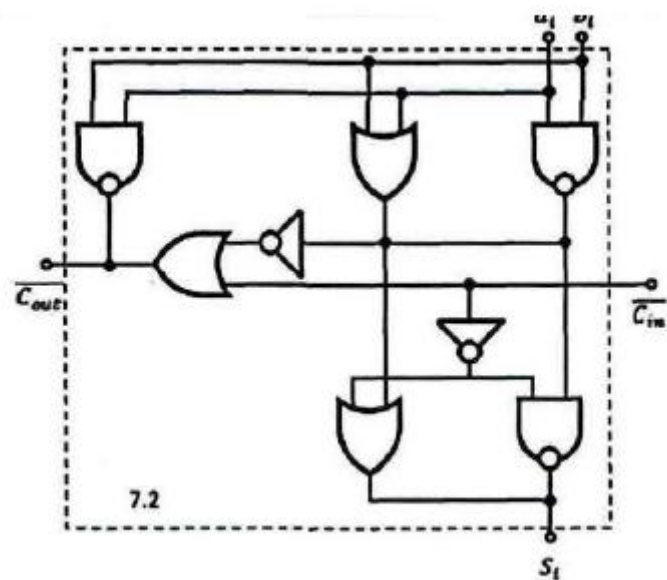
Пристрій для визначення ентропії, який містить аналого-цифровий перетворювач (АЦП), вхід якого з'єднаний з входом пристрою, синхронізатор, лічильники, шифратори та пірамідальний суматор, при цьому вхід АЦП з'єднаний з першими входами всіх парафазних компараторів, другі входи яких з'єднані з відповідними виходами взірцевих резисторів, другий вихід синхронізатора з'єднаний з другим входом пірамідального суматора та другими входами всіх лічильників, перші входи пірамідального суматора з'єднані з виходами відповідних шифраторів, а його вихід є виходом пристрою, в якому перший вихід синхронізатора з'єднаний з першими входами всіх лічильників, прямий вихід i -го компаратора у кожному каналі з'єднаний з третім входом i -го лічильника, інверсний вихід $(i+1)$ -го компаратора з'єднаний з четвертим входом i -го лічильника, виходи якого з'єднані з відповідними першими входами i -го регістра пам'яті, другий вхід всіх регістрів пам'яті з'єднаний з другим виходом синхронізатора, який **відрізняється** тим, що у кожному i -му каналі пристрою додатково введено два $(k-1)$ -розрядні двійкові лічильники, j -к-входи яких, відповідно, з'єднані з прямими виходами i -тих компараторів та інверсними виходами $(i+1)$ -тих компараторів, а виходи, відповідно, з'єднані з входами додатково введених 1-го та 2-го $(k-1)$ -розрядних регістрів пам'яті, виходи яких додатково з'єднані з відповідними входами додатково введеного k -розрядного двійкового суматора, виходи якого додатково з'єднані з входами i -го шифратора, а входи синхронізації других $(k-1)$ -розрядних лічильників з'єднані між собою та додатково введеним третім виходом синхронізатора.



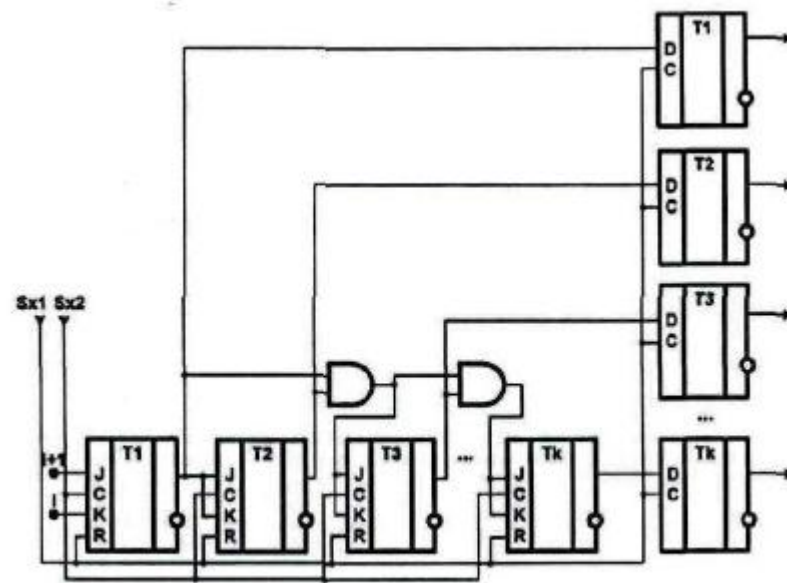
Фиг. 1



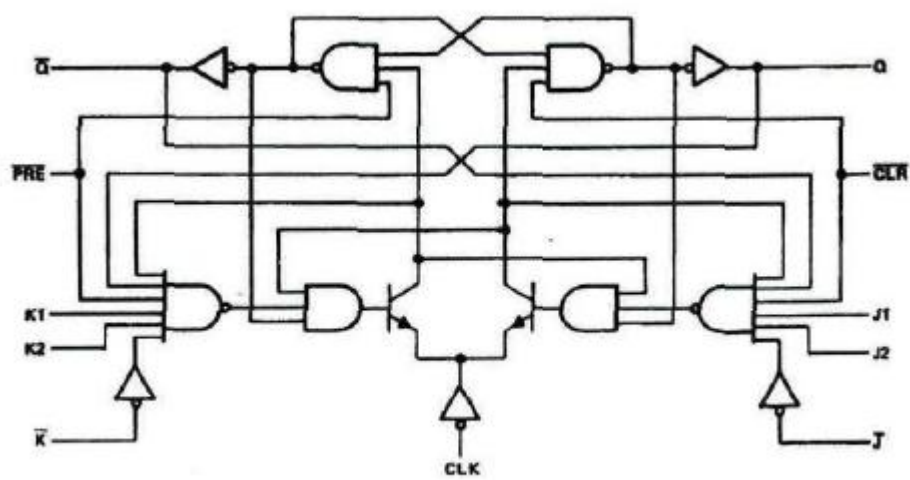
Фиг. 2



Фиг. 3



Фиг. 4



Фиг. 5

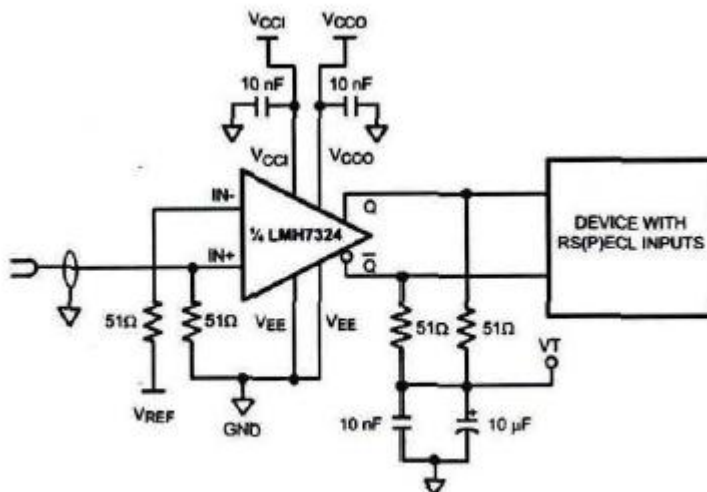


Fig. 6