ROMÂNIA

(19) OFICIUL DE STAT
PENTRU INVENŢII ŞI MĂRCI
Bucureşti

(11) **RO 135239 A0**
(51) Int.Cl.
G06F 7/58 (2006.01)

(12) # CERERE DE BREVET DE INVENŢIE

(21) Nr. cerere: **a 2021 00018**

(22) Data de depozit: **22/01/2021**

(41) Data publicării cererii:
30/09/2021 BOPI nr. **9/2021**

(71) Solicitant:
• **FUIOREA AUREL**, *NR.7C, LOCALITATEA IEZURENI, TÂRGU-JIU, GJ, RO*

(72) Inventatori:
• **FUIOREA AUREL**, *NR.7C, LOCALITATEA IEZURENI, TÂRGU-JIU, GJ, RO*

(54) # GENERATOR OPTIC DE NUMERE REAL-ALEATOARE

(57) **Rezumat:**

Invenţia se referă la un dispozitiv generator de numere real-aleatoare utilizat în aplicaţii ce privesc securitatea informaţiei şi/sau criptografia digitală. Dispozitivul conform invenţiei cuprinde un motor (**1**) electric care roteşte un disc (**4**) rotativ a cărui suprafaţă este împărţită în mai multe sectoare de cerc colorate diferit, un bloc (**5**) de senzori optici analogici reflexivi care măsoară reflectivitatea într-o anumită zonă a discului (**4**) rotativ şi un microcontroler (**3**) care acţionează motorul (**1**) electric prin intermediul unui motor-driver (**2**), prelucrează valorile transmise de senzorii optici şi transmite printr-un port USB numerele real-aleatoare rezultate.

Revendicări: 5
Figuri: 5

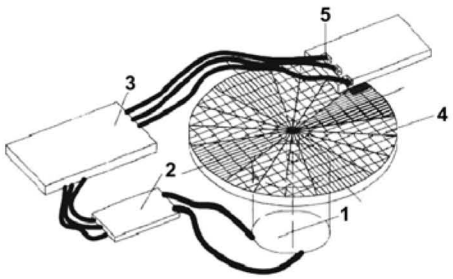

Fig. 1

Cu începere de la data publicării cererii de brevet, cererea asigură, în mod provizoriu, solicitantului, protecţia conferită potrivit dispoziţiilor art.32 din Legea nr.64/1991, cu excepţia cazurilor în care cererea de brevet de invenţie a fost respinsă, retrasă sau considerată ca fiind retrasă. Întinderea protecţiei conferite de cererea de brevet de invenţie este determinată de revendicările conţinute în cererea publicată în conformitate cu art.23 alin.(1) - (3).

RO 135239 A0

OFICIUL DE STAT PENTRU INVENŢII ŞI MĂRCI
Cerere de brevet de invenţie
Nr. a 2021 00018
Data depozit 22-01-2021

RO 135239 A0

27

GENERATOR OPTIC DE NUMERE REAL-ALEATOARE

Invenţia se referă la un dispozitiv ce generează numere real-aleatoare folosind un procedeu ce se bazează pe un fenomen fizic de natură optică, utilizat în aplicaţii ce privesc securitatea informaţiei si/sau criptografie digitală.

Arhitectura generală a unui generator de numere real-aleatoare este următoarea:

- sursa de entropie – generează un semnal ce este rezultatul unui fenomen fizic nedeterminist.
- digitizor – eşantionează periodic semnalul generat de sursa de entropie, convertind acest semnal într-o secvenţă de biţi aleatori.
- post-procesor – prelucrează informaţia (secvenţa de biţi aleatori) .

Pentru asigurarea securităţii fizice, este foarte util ca generatorul de numere real-aleatoare să fie compact, implementat într-un singur dispozitiv electronic care să conţină componentele esenţiale: sursa de entropie şi digitizorul.

Problema tehnică pe care o rezolvă invenţia este realizarea unui generator de numere real-aleatoare într-un dispozitiv portabil, uşor de realizat şi utilizat, având o sursă de entropie bună (bazată pe un fenomen fizic de natură optică), simplă şi care să aibă o cât mai mare aplicabilitate practică, putând fi conectat la o mare diversitate de aparate electronice sau lucrând independent pentru crearea tabelelor de numere real-aleatoare.

Procedeul şi dispozitivul propus exploatează următoarea caracteristică a senzorilor optici analogici reflexivi: valoarea tensiunii generată de senzor variază in funcţie de cantitatea de lumină IR reflectată de suprafaţa deasupra căreia se află senzorul (receptorul IR) in momentul când acesta realizează o măsurătoare (i.e. valoarea ce poate fi generată de senzor variază intre 0 si 1023, in funcţie de culoarea suprafeţei ce reflectă lumina IR generată de LED-ul IR al senzorului). Deasemenea, in apropierea interfeţelor suprafeţelor colorate diferit, având reflectanţă diferită, atunci când luminozitatea este puternică, apare fenomenul de duplicare a imaginii (ghosting) datorat reflexiilor interne dintre senzorul IR şi suprafaţa lucioasă reflectantă, ce creşte gradul de entropie al valorilor transmise de senzori.

Dispozitivul propus este alcătuit dintr-un motor electric ce roteşte un disc impărţit in foarte multe sectoare de cerc colorate diferit, un set de senzori optici analogici reflexivi ce măsoară reflectanţa sectoarelor colorate (ale discului ce se

roteşte) deasupra cărora se află, şi un microcontroler ce controlează turaţia motorului electric şi prelucrează valorile transmise de senzorii optici analogici reflexivi conform unui algoritm particular (i.e. valorile generate la un anumit moment de senzorii optici analogici reflexivi sunt înmulţite, valoarea rezultată fiind trunchiată modulo 256). Dacă se doreşte obţinerea de caractere aleatoare (e.g. pentru a fi utilizate în practica criptării), atunci numărul rezultat poate fi convertit de către microcontroler in caracterul ASCII corespunzător.

De asemenea, dispozitivului i se poate specifica (printr-o comandă) câte numere/caractere aleatoare să genereze intr-o sesiune .

Prelucrarea valorile transmise de senzorii optici analogici reflexiv făcută de microcontroler prin inmulţirea valorilor citite e făcută pentru a se obţine un număr aleatoriu (intervalul valorilor generate de dispozitiv este constant , numerele generate iau valori intre 0 şi 255) . Deci rolul inmulţirii este de obscurizare (i.e. in programare in mediul C, in cazul valorilor de tip UNSIGNED are loc o trunchiere atunci când este atinsă limita superioară ,255 in cazul nostru, rezultatul inmulţirii va fi tot timpul o valoare intre 0 si 255).

Sursa de entropie este determinată de mai mulţi parametri fizici, precum: viteza de rotaţie a axului motorului electric, unghiul la care se realizează citirea culorii, fluctuaţia luminii mediului ambiant, faptul că senzorii nu se poziţionează toţi exact pe anumite sectoare de culoare .

Aceasta invenţie prezintă următoarele avantaje:

- calitate ridicată - generatorul furnizează secvenţe de numere real-aleatoare de înaltă calitate;
- portabilitate - generatorul poate transmite numere real-aleatoare oricărui dispozitiv echipat cu un port USB;
- simplitate - generatorul este uşor de utilizat/configurat (plug-and-play), este simplu de realizat;
- consumă foarte puţină energie şi ocupă un spaţiu redus.

Dispozitivul are următoarele componente (Figura 1): motor electric (1) acţionat prin intermediul unui motor-driver (2) de către un microcontroler (3) care de asemenea comandă blocul de senzori optici (5) şi prelucrează valorile generate de aceştia in urma măsurării reflectanţei discului rotativ (4).

Viteza de generare a numerelor real–aleatoare poate fi crescută prin realizarea de sectoare de cerc colorate diferit pe ambele părţi ale discului rotativ (4) (Figura 2) şi citirea valorilor reflectanţei discului rotativ de către două blocuri de senzori optici analogici reflexivi (5),(6) poziţionate pe ambele feţe ale discului ..

Dispozitivul poate să aibă in componenţă mai multe blocuri de senzori optici care citesc valorile reflectanţei discului rotativ (4), aceste blocuri fiind poziţionate pe una sau ambele feţe ale discului rotativ. Sectoarele de cerc colorate , aflate pe disc pot fi inlocuite cu pete de culori şi forme diferite, ce acoperă toată suprataţa discului.

In Figura 3 este ilustrată implementarea generatorului de numere real-aleatoare propus, ca vedere din faţă , iar in Figura 4 este prezentată o vedere de sus a acestuia.

Implementarea propusă in Figura 1 are mai mulţi parametrii :

- viteza de rotaţie a motorului electric (1) (peste 200 rotaţii/secundă, preferabil de ordinul miilor de rotaţii) , acţionat prin intermediul unui motor-driver (2) de către un microcontroler (3) care de asemenea comandă blocul de senzori optici (5) format din 3 senzori optici (număr impar) şi prelucrează valorile generate de acestia in urma măsurării reflectanţei discului rotativ (4) , disc ce contine un număr foarte mare de sectoare de cerc colorate distinct (număr par, propus 28 culori);
- intervalul de pauză intre citiri de către blocul de senzori optici analogici (număr prim, cât mai mic posibil pentru obţinerea unui debit maxim) . De preferinţă, durata predefinită a pauzei (necesară sincronizării senzorilor) se situează în intervalul de la 1 milisecunde la 53 milisecunde, propus 3 milisecunde.

Se poate creşte mai mult gradul de entropie al sursei, conform Figura 5 , prin aplicarea unui capac transparent(7) deasupra discului rotativ(4) si umplerea spaţiului dintre capac si suprafaţa divers colorată a discului cu granule sferice (8) ce au culori diverse dar aceasi densitate, caz in care pe disc sunt dispuse forme (şicane) (9) ce imprăştie uniform granulele in mişcarea de rotaţie executată de disc (4). In Figura 5 sunt prezentate : un motor electric vibrator (1) ce este acţionat prin intermediul unui motor-driver (2) de către un microcontroler (3), care de asemenea comandă blocul de senzori optici (5) şi prelucrează valorile generate de aceştia in urma măsurării reflectanţei discului rotativ (4). Amestecarea şi distribuirea neuniformă a granulelor colorate divers va fi asigurată de motorul electric utilizat (care in acest caz trebuie să producă vibraţiile necesare amestecării granulelor) , de forta centrifugă generată de

mişcarea de rotaţie şi de sistemul de forme profilate pe disc, ce asigură o intindere a granulelor pe toată suprafaţa discului . Senzorii optici care citesc valorile reflectanţei vor transmite valori diverse deoarece lumina reflectată va fi influenţată si de punctele de culoare ale granulelor, nu numai de culoarea sectorului de cerc.

Dispozitivul propus poate fi utilizat în aplicaţii ce privesc securitatea informaţiei şi/sau criptografie digitală, acesta fiind de preferat algoritmilor software (care generează numere pseudo-aleatoare) deoarece generează numere real-aleatoare si de către producătorii de jocuri electronice / digitale. Deasemenea dispozitivul se poate conecta serial (prin ieşirea serial a microcontrolerului) la alte dispozitive al căror software necesită numere real-aleatoare generate.

REVENDICARI

1. Un procedeu pentru generarea de numere real-aleatoare utilizând valori generate de un bloc de senzori optici analogici-reflexivi ce măsoară reflexivitatea suprafeţelor divers colorate ale unor sectoare de cerc de pe faţa unui disc care este acţionat de un micro-motor electric, comanda micro-motorului, citirea şi prelucrarea valorilor transmise de senzorii optici analogici-reflexivi şi transmiterea printr-un port serial (USB) a numerelor real-aleatoare rezultate fiind realizată de acelaşi microcontroler.

2. Un procedeu pentru generarea de numere real-aleatoare utilizând valori generate de mai multe blocuri de senzori optici analogici-reflexivi ce măsoară reflexivitatea unui disc impărţit in sectoare de cerc divers colorate care este acţionat de un micro-motor electric, comanda micro-motorului, citirea şi prelucrarea valorilor transmise de senzorii optici analogici-reflexivi şi transmiterea printr-un port serial (USB) a numerelor real-aleatoare rezultate fiind realizată de acelaşi microcontroler.

3. Un dispozitiv ce generează numere real-aleatoare utilizând valori generate de un bloc de senzori optici analogici-reflexivi ce măsoară reflexivitatea unui disc impărţit in sectoare de cerc divers colorate care este acţionat de un micro-motor electric, comanda micro-motorului, citirea şi prelucrarea valorilor transmise de senzorii optici analogici-reflexivi şi transmiterea printr-un port serial (USB) a numerelor real-aleatoare rezultate fiind realizată de acelaşi microcontroler.

4. Un dispozitiv ce generează numere real-aleatoare utilizând valori generate de mai multe blocuri de senzori optici analogici-reflexivi ce măsoară reflexivitatea unui disc impărţit in sectoare de cerc divers colorate care este acţionat de un micro-motor electric, comanda micro-motorului, citirea şi prelucrarea valorilor transmise de senzorii optici analogici-reflexivi şi transmiterea printr-un port USB a numerelor real-aleatoare rezultate fiind realizată de acelaşi microcontroler.

5. Dispozitiv conform oricăreia dintre revendicările 3. şi 4. în care discul cu suprafeţe divers colorate este acoperit parţial de granule colorate diferit si este acţionat de un micro-motor electric ce produce şi vibraţii la rotire , necesare amestecării continue a granulelor.

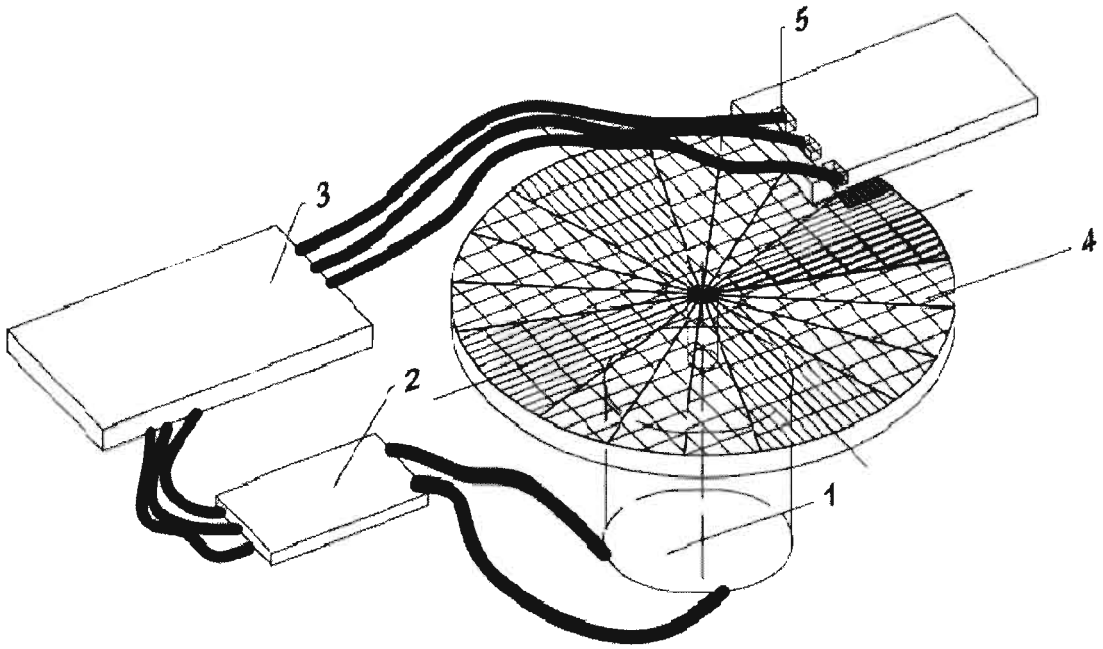

Figura 1.

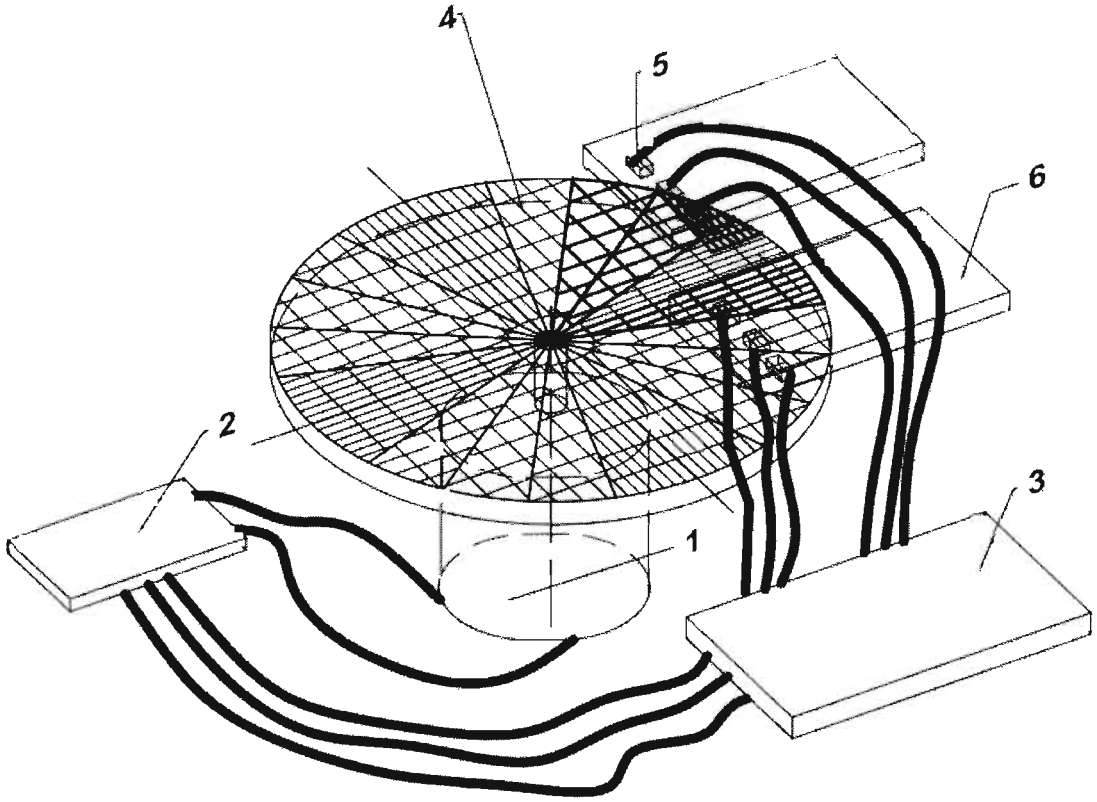

Figura 2

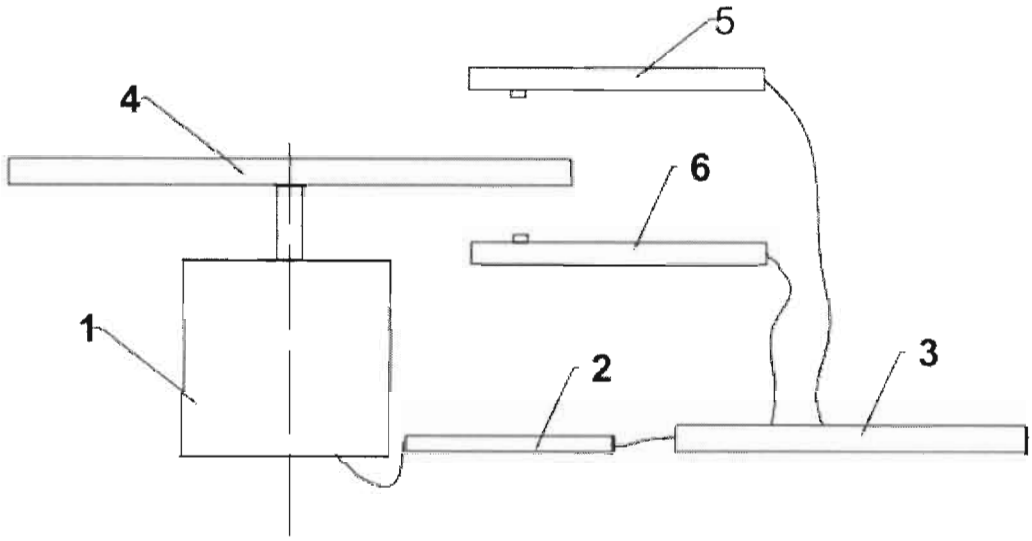

Figura 3

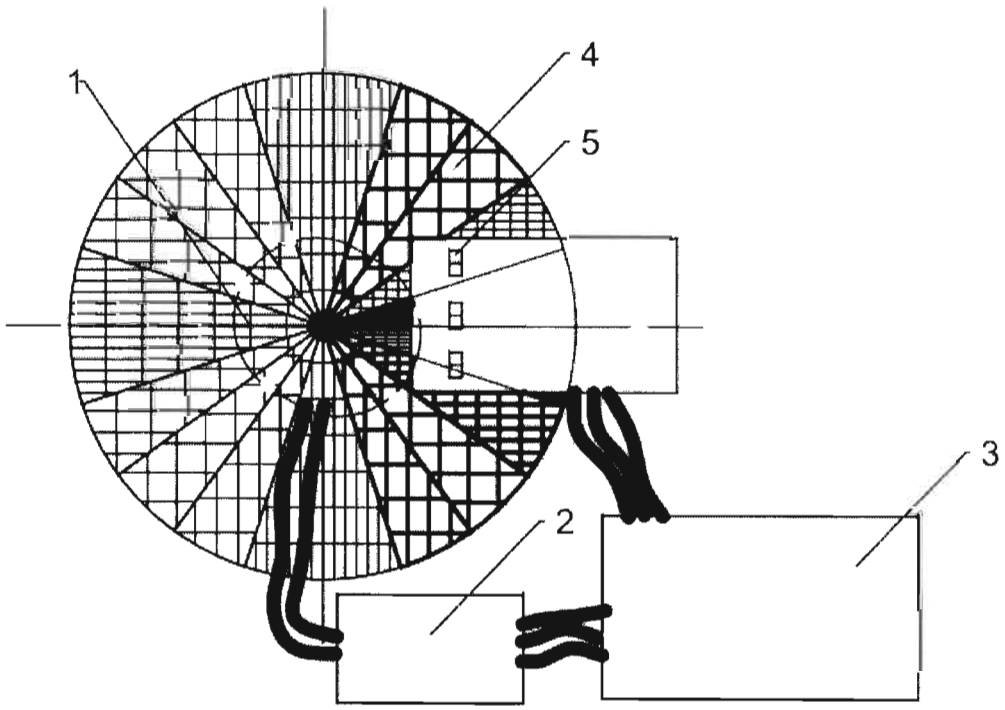

Figura 4

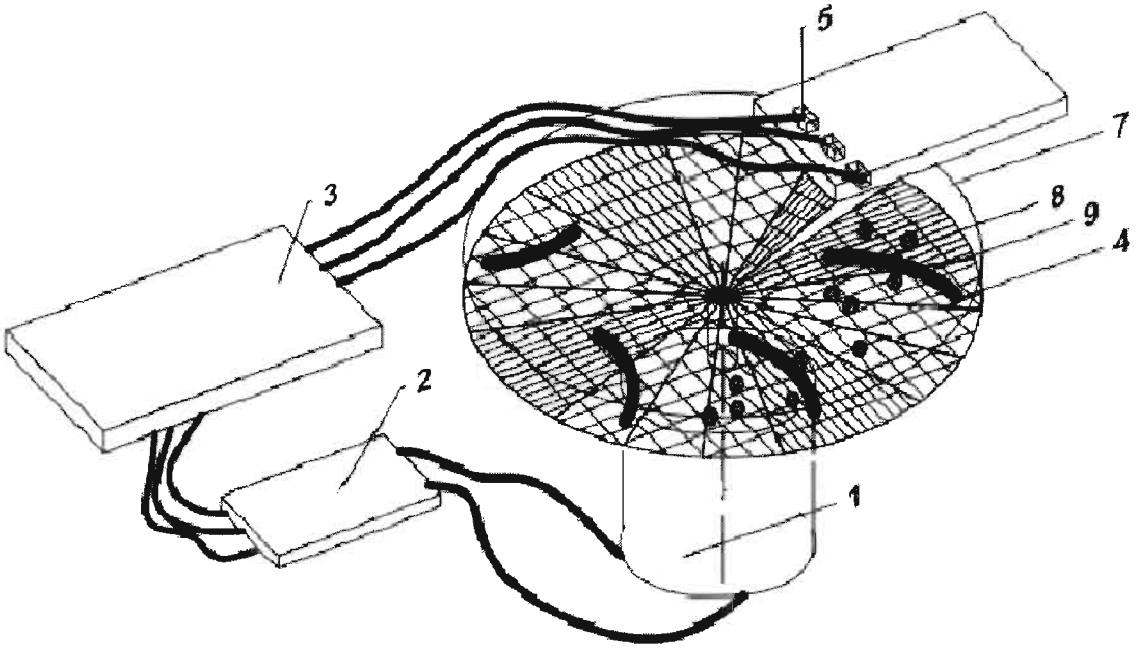

Figura 5.