(19) URZĄD PATENTOWY RZECZYPOSPOLITEJ POLSKIEJ

(10) **PL 245872 B1**

(12) # Opis patentowy

(21) Numer zgłoszenia: **440695**
(22) Data zgłoszenia: **2022.03.18**
(43) Data publikacji o zgłoszeniu: **2023.09.25 BUP 39/2023**
(45) Data publikacji o udzieleniu patentu: **2024.10.21 WUP 43/2024**

(51) MKP:
G06F 7/58 *(2006.01)*

(73) Uprawniony z patentu:
UNIWERSYTET WARSZAWSKI, Warszawa, PL
UNIWERSYTET GDAŃSKI, Gdańsk, PL

(72) Twórca(-y) wynalazku:
MARCIN PAWŁOWSKI, Gdynia, PL
MICHAŁ JACHURA, Warszawa, PL
MARCIN JARZYNA, Warszawa, PL
KONRAD BANASZEK, Warszawa, PL
KAROL ŁUKANOWSKI, Warszawa, PL

(74) Pełnomocnik:
rzecz. pat. Cezary Samojłowicz, Warszawa, PL

(54) Tytuł:
Urządzenie do kwantowej generacji liczb losowych oparte na polaryzacji światła oraz sposób weryfikacji prywatności sekwencji liczb losowych generowanych za pomocą tego urządzenia

PL 245872 B1

Opis wynalazku

[Dziedzina techniki]

Przedmiotem wynalazku jest urządzenie do kwantowej generacji liczb losowych oparte na polaryzacji światła oraz sposób weryfikacji prywatności sekwencji liczb losowych, generowanych za pomocą urządzenia do kwantowego generowania liczb losowych. Generacja losowych ciągów liczb odbywa się poprzez pomiar kwantowych stanów koherentnych, lub kwantowych stanów Focka za pomocą pary detektorów pojedynczych fotonów. Rejestracja wyników pomiarów pozwala na otrzymanie prawdziwie losowej sekwencji bitów, która w razie potrzeby może być konwertowana na zbiór prawdziwie losowych liczb w zapisie dziesiętnym. Weryfikacja prywatności realizowana jest za pomocą umieszczonego w generatorze wielostanowego modulatora polaryzacji lub pary dwustanowych modulatorów polaryzacji modyfikujących mierzony stan kwantowy.

[Stan techniki]

Generacja liczb losowych znajduje szerokie zastosowanie w takich dziedzinach techniki jak klasyczna i kwantowa kryptografia, komputerowe symulacje numeryczne (metoda Monte Carlo), jak również stanowi podstawę działania internetowych kasyn i loterii. Generatory liczb losowych w zależności od zasady działania dzielą się na generatory liczb pseudolosowych (*ang. pseudorandom number generator*), w których komputerowy algorytm na podstawie krótkiego zbioru liczb losowych, tzw. ziarna (*ang. seed*), w sposób deterministyczny generuje ciąg liczb o cechach zbliżonych do losowych oraz generatory liczb prawdziwie losowych (*ang. true random number generator*), w których liczby losowe generowane są na podstawie inherentnie losowego zjawiska fizycznego (np. rozpadu radioaktywnego [K. Park, S Park, B. G. Choi, T. Kang, J. Kim, Y.-H, Kim, H.-Z. Jin, "A lightweight true random number generator using beta radiation for IoT applications", ETRI Journal. 42(6), 951–964 (2020)] albo elektromagnetycznego szumu atmosferycznego [https://www.random.org/]). Generatory pseudolosowe mają szereg wad związanych z cyklicznością generowanych liczb oraz niejednorodnością ich rozkładu. Dodatkowo w przypadku przechwycenia ziarna przez osobę nieuprawnioną, może ona wygenerować taką samą sekwencję liczb bez wiedzy użytkownika generatora, stwarzając poważne zagrożenie dla prywatności sekwencji.

Dzięki probabilistycznej naturze pomiaru w mechanice kwantowej, wykorzystanie zjawisk kwantowych do generacji liczb prawdziwie losowych stało się naturalnym kierunkiem rozwoju szybkich, tanich i zminiaturyzowanych generatorów. W pracy [X. Ma, X. Yuan, Z. Cao, B. Qi, Z, Zhang "Quantum random number generation" npj Quantum Information 2, 16021 (2016)] przedstawiono przegląd najważniejszych eksperymentów wykonanych w ciągu ostatnich 20 lat, w których do generacji liczb prawdziwie losowych wykorzystywane są zjawiska optyki kwantowej takie jak pomiar wzmocnionej emisji spontanicznej, pomiar kwantowych fluktuacji próżni oraz pomiar stanu kwantowego pojedynczego fotonu. Perfekcyjna losowość kwantowych generatorów liczb losowych oraz prywatność generowanej przez nie sekwencji wynika z uproszczonych modeli teoretycznych, które zakładają wyidealizowany scenariusz, w którym użytkownik posiada pełną wiedzę na temat budowy urządzenia, komponenty optyczne mają niezmienne w czasie parametry, a podczas pomiaru nie występują błędy pomiarowe etc. Działanie realistycznych generatorów zawsze jednak wykazuje pewne odstępstwa od modelu teoretycznego spowodowane m.in. fluktuacjami temperatury, zużyciem elementów optycznych i elektronicznych, jak również; w najgorszym scenariuszu intencjonalną ingerencją producenta bądź innej strony nieuprawnionej w urządzenie. W celu odróżnienia, czy urządzenie generuje predefiniowaną sekwencję losowych liczb „znaną przez producenta bądź innej strony nieuprawnionej, czy też jest to generowana w czasie rzeczywistym prywatna sekwencja (to znaczy taka, która nie może być odgadnięta lub zrekonstruowana przez stronę nieuprawnioną), konieczne jest opracowanie procedury testowania (certyfikacji) takiego urządzenia. Procedura testowania jest niezbędna zwłaszcza w przypadku gdy urządzenie kupowane jest od zewnętrznej firmy, w związku z czym użytkownik nie posiada pełnej wiedzy na temat jego budowy i musi je traktować jako niezaufane.

Kwantowe generatory liczb losowych testujące podczas swojego działania prywatność i losowość generowanej sekwencji (generatory samotestujące) stanowią najbezpieczniejszą klasę urządzeń o najszerszych możliwościach aplikacyjnych. Ta najbezpieczniejsza klasa urządzeń nazywana jest klasą niezależną sprzętowo (*ang. device independent quantum random number generator*). Jedna z pierwszych realizacji takiego urządzenia została opisana w pracy [A. Kulikov, M. Jerger, A. Potočki, A. Wallraff, A. Fedorov "Realization of Quantum Random Generator Certified with the Kochen-Specker Theorem"

Phys. Rev. Lett. **119**, 240501 (2017)], gdzie testowanie jest realizowane za pomocą twierdzenia Kochena-Speckera, zaś osiągana prędkość generacji losowych bitów sięga 25 kbit/s.

W pracy [D. Drahi i inni "Certified Random Numbers from Untrusted Light" Phys. Rev. X 10, 041048 (2020)] opisano rekordowo szybki (8.21 Gbit/s), częściowo samotestujący generator liczb losowych oparty na optycznym homodynym pomiarze kwantowych fluktuacji próżni. Generator ten składa się z lasera pracy ciągłej, atenuatora optycznego o regulowanym tłumieniu, kostek światłodzielących, szybkich fotodiod oraz elektroniki sterującej. Część wiązki optycznej w generatorze wykorzystywana jest do testowania przychodzącego stanu koherentnego wytwarzanego przez laser, dzięki czemu może on korzystać z niezaufanego źródła światła. Układ pomiarowy w generatorze nie jest testowany, w związku z czym jego implementacja wymaga użycia zaufanych fotodetektorów. Tym samym jest to generator częściowo samotestujący należący do klasy bezpieczeństwa nazywanej klasą niezależną źródłowo (ang. *source device independent*).

W zgłoszeniu US20190393675A1 opisano generator liczb losowych, w którym optyczny pomiar homodynowy wykonuje się na zewnętrznej wiązce światła doprowadzanej niezależnie do urządzenia przez użytkownika. Faza lokalnego oscylatora w pomiarze homodynowym może być ustalona lub losowa. Pozwala to na pomiar różnych kwadratur zewnętrznej wiązki światła będącej np. w stanie ściśniętym, stanie koherentnym, lub w stanie próżni: Dzięki pomiarowi zewnętrznego stanu światła rozwiązanie to pozwala na testowanie układu pomiarowego w generatorze. Zaufane źródło światła, niezbędne do działania generatora, musi być natomiast niezależnie zakupione i przetestowane lub samodzielnie skonstruowane przez użytkownika. W związku z tym jest to generator częściowo samotestujący należący do klasy bezpieczeństwa nazywanej klasą niezależną pomiarowo (ang. *measurement device independent*).

W zgłoszeniu WO2018065593A1 przedstawiono kwantowy generator liczb losowych oparty na pomiarze bezpośrednim dwóch nieortogonalnych stanów światła w parze modów czasowych tj. $|0\rangle_{t1}|\alpha\rangle_{t2}$ oraz $|\alpha\rangle_{t1}|0\rangle_{t2}$. Pomiar wykonywany jest za pomocą detektora pojedynczych fotonów wyposażonego w rozdzielczością czasową. Iloczyn skalarny dwóch nieortogonalnych stanów zadany funkcją $e^{-|\alpha|^2}$, może być modyfikowany w generatorze poprzez zmianę amplitudy stanów koherentnych. Pozwala to na przetestowanie stanów światła, na podstawie których generowane są liczby losowe. Detektor umożliwiający pomiar pojedynczych fotonów z rozdzielczością czasową musi być zaufany. Tym samym jest to generator częściowo samotestujący należący do klasy bezpieczeństwa nazywanej klasą niezależną źródłowo (ang. *source device independent*).

W zgłoszeniu WO2021215941A1 przedstawiono samotestujący generator liczb losowych zbudowany w oparciu o wieloportowe dzielniki wiązki (ang. *multiport beam splitter*), modulatory fazy oraz zestaw detektorów pojedynczych fotonów. Jeden zestaw modulatorów fazy wykorzystywany jest do modyfikowania stanu wychodzącego ze źródła światła, zaś drugi zestaw modulatorów fazy do modyfikowania stanu wchodzącego do układu detekcji bazującego na wieloportowym dzielniku wiązki. Dzięki takiej architekturze generatora, możliwe, jest niezależne testowanie zarówno stanów światła na podstawie których generowana jest losowość jak również układu detektorów. Układ ten jest bardzo trudny w praktycznej realizacji ze względu na konieczność utrzymania stabilności fazowej między wieloma wiązkami światła interferującymi ze sobą wewnątrz wieloportowego dzielnika wiązki. Dodatkowe problemy stwarza wykorzystanie optycznych modulatorów fazy które dla stabilnego działania wymagają precyzyjnej kalibracji punktu pracy i kontrolowanych warunków środowiskowych takich jak temperatura.

W stanie techniki znane są detektory pojedynczych fotonów działające w oparciu o zjawisko nadprzewodnictwa [Erie A. Dauler i inni Review of superconducting nanowire single-photon detector system design options and demonstrated performance, Optical Engineering 53(8), 081907 (2014)]. Detektory takie cechują się niezwykle niską liczbą ciemnych zliczeń oraz bardzo wysoką wydajnością kwantową pozwalającą na efektywną detekcję fotonów.

[Problem ze stanu techniki]

Problemem ze stanu techniki jest zaprojektowanie i budowa kwantowego generatora liczb prawdziwie losowych, w którym losowość generowana jest na podstawie inherentnie probabilistycznego zjawiska fizycznego, zaś generowany ciąg liczb losowych z całkowitą pewnością nie będzie znany stronie nieuprawnionej, włączając w to producenta generatora, tzn. generator zapewnia prywatność sekwencji. Osobnym problemem ze stanu techniki jest implementacja takiego generatora za pomocą możliwie najprostszego w budowie układu optycznego składającego się z powszechnie dostępnych i tanich elementów optycznych i optoelektronicznych.

[Słownik i definicje znanych w stanie techniki zwrotów wykorzystanych w opisie]

W niniejszym opisie stosowane terminy mają następujące znaczenia, opisane w definicjach poniżej:

Termin “bity losowe” oznacza bity generowane przez wynalazek tworzące prawdziwie losowy ciąg bitów wyjściowych.

Termin “bit prywatny” oznacza bit generowany przez urządzenie, który nie może być odgadnięty lub zrekonstruowany przez stronę nieuprawnioną włączając w to producenta generatora.

Termin “bity sterujące” oznacza bity sygnału cyfrowego podawanego na wejście elektryczne modulatora/ów polaryzacji.

Termin “detektor pojedynczych fotonów” odnosi się do urządzenia, pozwalającego na detekcję światła o energii odpowiadającej energii pojedynczego fotonu optycznego. Przykładem takich detektorów są m in. fotodiody lawinowe, SPD (ang. *single photon detector*) oraz nadprzewodnikowe nanoprzewodowe detektory pojedynczych fotonów.

Termin “element separujący polaryzacje” oznaczony na figurach rysunku jako 110, oznacza element optyczny, w którym polaryzacja pionowa wiązki optycznej jest transmitowana, zaś polaryzacja pozioma wiązki optycznej odbijana. Przykładami takiego elementu są kostki dzielące polaryzację z powloką dielektryczną (PBS – ang. *polarizing beam splitter*) oraz polaryzatory oparte na dwójłomności (np. pryzmat typu Wollaston, pryzmat typu Nicola, pryzmat typu Glan-Taylor, pryzmat typu Glan-Thompson),

Termin “generator samotestujący” oznacza generator liczb losowych testujący podczas swojego działania prywatność generowanej sekwencji.

Termin “kliknięcie” oznacza w kontekście detektora pojedynczych fotonów wygenerowanie impulsu elektrycznego/elektronicznego w odpowiedzi na zarejestrowany foton lub spontaniczne wygenerowanie impulsu elektrycznego/elektronicznego związanego z ciemnym zliczeniem (ang. *dark count*).

Termin “moduł generujący” oznacza układ elektroniczny generujący bit *0* gdy detektor 131 rejestruje zliczenie oraz bit *1* gdy detektor 132 generuje zliczenie. Moduł 140 umożliwia generowanie losowej sekwencji bitów na wyjściu cyfrowym 143. Moduł taki może bazować na powszechnie dostępnych mikrokontrolerach lub bezpośrednio programowalnych macierzach bramek (ang. *field-programmable gate array, FPGA*).

Termin “polaryzacja pionowa” oznacza kierunek polaryzacji liniowej, taki że wiązka optyczna o tej polaryzacji jest transmitowana przez element separujący polaryzacje.

Termin “polaryzacja pozioma” oznacza kierunek polaryzacji liniowej, taki że wiązka optyczna o tej polaryzacji jest odbijana przez element separujący polaryzacje.

Termin “polaryzacja ukośna” oznacza kierunek polaryzacji liniowej, taki że wiązka optyczna o tej polaryzacji jest równo dzielona przez element separujący polaryzacje na dwie wiązki optyczne o równych energiach, przy czym wiązka odbijana jest spolaryzowana poziomo, zaś wiązka transmitowana jest spolaryzowana pionowo.

Termin “prywatność sekwencji” oznacza, że sekwencja bitów generowanych przez urządzenie nie może być odgadnięta lub zrekonstruowana przez stronę nieuprawnioną włączając w to producenta generatora.

Termin “strona nieuprawniona” oznacza każdą osobę lub instytucję, która w sposób nieuprawniony i bez wiedzy użytkownika, próbuje uzyskać informację o generowanej sekwencji liczb losowych, a tym samym złamać prywatność sekwencji. Stronami nieuprawnionymi mogą być potencjalny podsłuchiwacz, producent urządzenia, dostawca oprogramowania lub inna strona niebędąca użytkownikiem urządzenia.

Termin “układ sterujący” oznacza układ elektryczny generujący cyfrowy lub analogowy sygnał sterujący wielostanowym modulatorem polaryzacji lub parą dwustanowych modulatorów polaryzacji. Układ taki może bazować na powszechnie dostępnych mikrokontrolerach lub bezpośrednio programowalnych macierzach bramek (ang. *field-programmable gate array, FPGA*).

Termin “weryfikacja prywatności” oznacza sprawdzenie, czy maksymalne prawdopodobieństwo odgadnięcia losowego bitu przez stronę nieuprawnioną P_g jest mniejsze niż maksymalna akceptowalna wartość prawdopodobieństwa X, gdzie X przyjmuje wartości w zakresie od 50% do 100%. Weryfikacja jest pozytywna gdy nierówności $P_g < X$ jest spełniona. Weryfikacja jest negatywna gdy nierówność $P_g < X$ nie jest spełniona. Dla strategii strony nieuprawnionej polegającej na odgadywaniu losowych bitów bez żadnej dodatkowej informacji maksymalne prawdopodobieństwo P_g wynosi 50%. Gdy weryfikacja jest pozytywna urządzenie jest zdolne do generowania losowych bitów prywatnych.

Termin "współczynnik ekstynkcji” dla elementu separującego polaryzacje określa stosunek energii wiązki optycznej transmitowanej przez element, do wiązki optycznej odbijanej przez element, gdy

wiązka padająca na element ma polaryzacje pionową. Przykładowo dla kostek dzielących polaryzację (PBS) współczynnik ekstynkcji wynosi 1000:1.

Termin "źródło światła" oznacza źródło światła koherentnego (np. dioda laserowa) lub źródło światła niekoherentnego (np. dioda LED), lub źródło pojedynczych fotonów (przykładowo oparte na pojedynczych atomach lub kropkach kwantowych). Centralna długość fali wiązki światła używanej w urządzeniu znajduje się w zakresie 400–1600 nm. Średnia moc optyczna wiązki światła używanej w urządzeniu jest mniejsza niż 1 μW.

Inne, niezdefiniowane powyżej terminy posiadają w niniejszym dokumencie znaczenia, które są podane i zrozumiane przez specjalistę w dziedzinie w świetle posiadanej najlepszej wiedzy, niniejszego ujawnienia i kontekstu opisu zgłoszenia patentowego.

[Rozwiązanie problemu ze stanu techniki]

Wynalazek opisany niniejszym dokumentem patentowym obejmuje nowatorską konstrukcję urządzenia oraz innowacyjny sposób samotestującej generacji liczb prawdziwie losowych opartych na prawach mechaniki kwantowej, generowanych za pomocą tego urządzenia. Urządzenie według wynalazku zawiera w swojej budowie jeden wielostanowy modulator polaryzacji lub parę dwustanowych modulatorów polaryzacji, dzięki którym użytkownik urządzenia posiada możliwość weryfikowania prywatności generowanych liczb losowych. Dzięki unikatowej konstrukcji urządzenia, pozwala ono na wykrycie ewentualnej ingerencji ze strony producenta urządzenia i/lub strony nieuprawnionej w proces generacji liczb prawdziwie losowych.

[Ujawnienie istoty wynalazku]

Przedmiotem wynalazku jest urządzenie do kwantowej generacji liczb losowych zawierające źródło światła 100 o ustalonej polaryzacji oraz połączony z nim torem optycznym element dzielący polaryzacje 110 mający pierwsze wyjście 111 odpowiadające polaryzacji pionowej i drugie wyjście 112 odpowiadające polaryzacji poziomej oraz pierwszy detektor 131 połączony torem optycznym z pierwszym wyjściem 111 elementu dzielącego polaryzacje 110 i drugi detektor 132 połączony torem optycznym z drugim wyjściem 112 elementu dzielącego polaryzacje 110, moduł generujący 140, mający pierwsze wejście 141 połączone z wyjściem pierwszego detektora 131 oraz drugie wejście 142 połączone z wyjściem drugiego detektora 132, oraz wyjście dwustanowe 143, przystosowany do generowania na wyjściu dwustanowym 143 bitów o wartości *1* po otrzymaniu sygnału na pierwszym wejściu 141 i bitów o wartości *0* po otrzymaniu sygnału na drugim wejściu 142, charakteryzujące się tym, że źródło światła 100 jest połączone z elementem dzielącym polaryzacje 110 za pośrednictwem wielostanowego modulatora polaryzacji 150 sterowanego sygnałem cyfrowym lub analogowym generowanym za pomocą elektronicznego układu sterującego 160 połączonego z wielostanowym modulatorem polaryzacji 150.

Korzystnie wielostanowy modulator polaryzacji 150, zawiera dwa połączone ze sobą torem optycznym dwustanowe modulatory polaryzacji 251 oraz 252 przy czym oba modulatory przystosowane są do obrotu polaryzacji o 45° gdy na ich wejście elektryczne podawany jest sterujący sygnał cyfrowy o wartości bitu *1* oraz do obrotu polaryzacji o 0° gdy na ich wejście elektryczne podawany jest sterujący sygnał cyfrowy o wartości bitu *0*, lub alternatywnie do obrotu polaryzacji o 45° gdy na ich wejście elektryczne podawany jest sterujący sygnał cyfrowy o wartości bitu *0* oraz do obrotu polaryzacji o 0° gdy na ich wejście elektryczne podawany jest sterujący sygnał cyfrowy o wartości bitu *1*.

Korzystnie wielostanowy modulator polaryzacji 150, zawiera dwa połączone ze sobą torem optycznym dwustanowe modulatory polaryzacji 351 oraz 352, przy czym jeden z modulatorów 351, 352 obraca polaryzację o 45° gdy na jego wejście elektryczne 5 podawany jest sygnał cyfrowy o wartości bitu *1* oraz obraca polaryzację o 0° gdy na jego wejście elektryczne podawany jest sygnał cyfrowy o wartości bitu *0*, zaś odpowiednio drugi z modulatorów 351, 352 obraca polaryzację o 90° gdy na jego wejście elektryczne podawany jest sygnał cyfrowy o wartości bitu *1* oraz obraca polaryzację o 0° gdy na jego wejście elektryczne podawany jest sygnał cyfrowy o wartości bitu *0*.

Korzystnie wielostanowy modulator polaryzacji 150, zawiera dwa połączone ze sobą torem optycznym dwustanowe modulatory polaryzacji 351 oraz 352, przy czym jeden z modulatorów 351, 352 obraca polaryzację o 45° gdy na jego wejście elektryczne podawany jest sygnał cyfrowy o wartości bitu *0* oraz obraca polaryzację o 0° gdy na jego wejście elektryczne podawany jest sygnał cyfrowy o wartości bitu *1*, zaś drugi z modulatorów, odpowiednio 351, 352 obraca polaryzację o 90° gdy na jego wejście elektryczne podawany jest sygnał cyfrowy o wartości bitu *0* oraz obraca polaryzację o 0° gdy na jego wejście elektryczne podawany jest sygnał cyfrowy o wartości bitu *1*. Korzystnie elementem separującym polaryzacje 110 jest kostka dzieląca polaryzacje z powłoką dielektryczną lub polaryzator oparty na dwójłomności lub pryzmat.

Korzystnie źródłem światła 100 jest źródło światła koherentnego, korzystnie zawierające diodę laserową lub laser impulsowy, lub źródło światła niekoherentnego korzystnie zawierające diodę LED, lub źródło pojedynczych fotonów, korzystnie oparte na pojedynczych atomach lub kropkach kwantowych.

Korzystnie źródło światła 100 jest przystosowane do emitowania impulsów światła o polaryzacji pionowej lub poziomej.

Korzystnie źródło światła 100 jest przystosowane do generowania wiązki optycznej o centralnej długości fali w zakresie 400–1600 nm, której średnia energia jest mniejsza niż 1 μW.

Korzystnie oba detektory pojedynczych fotonów 131 i 132 zawierają fotodiodę lawinową lub detektor pojedynczych fotonów oparty na nadprzewodnictwie, lub alternatywnie jeden z detektorów 131, 132 zawiera fotodiodę lawinową, zaś drugi z detektorów zawiera detektor pojedynczych fotonów oparty na nadprzewodnictwie.

Korzystnie torem optycznym jest światłowód, falowód lub wiązka optyczna w wolnej przestrzeni.

Przedmiotem wynalazku jest również sposób weryfikacji prywatności sekwencji bitów losowych generowanych za pomocą urządzenia do kwantowej generacji liczb losowych zawierającego źródło światła 100 o ustalonej polaryzacji oraz połączony z nim element dzielący polaryzacje 110 mający pierwsze wyjście 111 odpowiadające polaryzacji pionowej i drugie wyjście 112 odpowiadające polaryzacji poziomej, oraz pierwszy detektor 131 połączony z pierwszym wyjściem 111 elementu dzielącego polaryzacje 110 i drugi detektor 132 połączony z drugim wyjściem 112 elementu dzielącego polaryzacje 110, moduł generujący 140, mający pierwsze wejście 141 połączone z wyjściem pierwszego detektora 131 oraz drugie wejście 142 połączone z wyjściem drugiego detektora 132, oraz wyjście dwustanowe 143, przystosowany do generowania na wyjściu dwustanowym 143 bitów o wartości *1* po otrzymaniu sygnału na pierwszym wejściu 141 i bitów o wartości *0* po otrzymaniu sygnału na drugim wejściu 142, w układzie podczas generowania liczb losowych polaryzacja wiązki padającej na element separujący polaryzacje jest ukośna, czyli obrócona o 45° względem kierunku polaryzacji transmitowanego przez element separujący polaryzacje charakteryzujący się tym, że podczas weryfikacji prywatności za pomocą układu sterowania 160 steruje się wielostanowym modulatorem polaryzacji 150 i obraca się polaryzację światła padającego na element separujący polaryzacje 110, ustawiając ją kolejno pod kątem 0°, 45°, oraz 90° do kierunku polaryzacji transmitowanego przez element separujący polaryzacje oraz dla każdego z trzech kierunków polaryzacji (0°, 45°, 90°) rejestruje się sekwencje bitów generowanych przez moduł generujący 140, a następnie na podstawie każdej z trzech sekwencji wyznacza się prawdopodobieństwo zarejestrowania zliczenia przez pierwszy detektor 131 oraz prawdopodobieństwo zarejestrowania zliczenia przez drugi detektor 132 oraz na podstawie sześciu prawdopodobieństw $(P^{I}_{00}, P^{II}_{00}, P^{I}_{11}, P^{II}_{11}, P^{I}_{01}, P^{II}_{01}$ lub $P^{I}_{00}, P^{II}_{00}, P^{I}_{11}, P^{II}_{11}, P^{I}_{10}, P^{II}_{10}$ lub $P^{I}_{00}, P^{II}_{00}, P^{I}_{01}, P^{II}_{01}, P^{I}_{10}, P^{II}_{10}$ lub $P^{I}_{00}, P^{II}_{00}, P^{I}_{01}, P^{II}_{01}, P^{I}_{11}, P^{II}_{11}$ lub $P^{I}_{V_0}, P^{II}_{V_0}, P^{I}_{V_1}, P^{II}_{V_1}, P^{I}_{V_2}, P^{II}_{V_2})$ oblicza się parametry modelu fizycznego układu, które stosuje się do wyznaczenia maksymalnego prawdopodobieństwa odgadnięcia losowego bitu przez stronę nieuprawnioną P_g i weryfikację prywatności uznaje się za pozytywną jeżeli maksymalne prawdopodobieństwo odgadnięcia losowego bitu przez stronę nieuprawnioną P_g jest mniejsze niż maksymalna akceptowalna wartość prawdopodobieństwa odgadnięcia losowego bitu przez stronę nieuprawnioną X, gdy weryfikacja jest pozytywna urządzenie jest zdolne do generowania losowych bitów prywatnych.

Korzystnie do wyznaczenia maksymalnego prawdopodobieństwa odgadnięcia losowego bitu przez stronę nieuprawnioną P_g stosuje się model fizyczny, którego parametrami są:

(a) średnia liczba fotonów w mierzonych impulsach – μ;

(b) współczynnik transmisji – λ;

(c) prawdopodobieństwo – f.

Korzystnie weryfikację prywatności generowanej sekwencji bitów losowych uznaje się za pozytywną w zależności od przynależności wyznaczonych wartości parametrów modelu fizycznego (μ_0, λ_0, f_0) do predefiniowanego zbioru wartości liczbowych w przestrzeni trójwymiarowej (μ, λ, f) wyliczonego na podstawie modelu fizycznego oraz na podstawie maksymalnej akceptowalnej wartości prawdopodobieństwa odgadnięcia losowego bitu przez stronę nieuprawnioną X.

Korzystnie maksymalna akceptowalna wartość prawdopodobieństwa odgadnięcia losowego bitu przez stronę nieuprawnioną X znajduje się w przedziale od 50% do 100%.

Korzystnie maksymalna akceptowalna wartość prawdopodobieństwa odgadnięcia losowego bitu przez stronę nieuprawnioną X wynosi 75%, dla $X = 75\%$ weryfikacja prywatności generowanej sekwencji bitów losowych jest pozytywna (tj. $P_g < 75\%$), gdy wyznaczone wartości parametrów modelu fizycznego (μ_0, λ_0, f_0) znajdują się wewnątrz czworościanu, którego wierzchołki znajdują się w następujących punktach przestrzeni trójwymiarowej (μ, λ, f):

- *(μ=0, λ=0, f=0);*
- *(μ=0, λ=0,75, f=0);*
- *(μ=10, λ=0, f=0);*
- *(μ=0, λ=0, f=1).*

Przedmiotem wynalazku jest także produkt komputerowy, charakteryzujący się tym, że zawiera oprogramowanie, które po wgraniu do układu sterującego 160 i modułu generującego 140 realizuje sposób zgodny z opisanym wynalazkiem.

[**Zalety wynalazku**]

Wynalazek według niniejszego opisu patentowego posiada liczne zalety. Pozwala on na generację liczb prawdziwie losowych, dając jednocześnie całkowitą pewność, że generowana sekwencja liczb losowych nie jest znana stronie nieuprawnionej włączając w to producenta generatora. Dzięki wykorzystaniu polaryzacyjnego stopnia swobody jego techniczna realizacja jest dużo prostsza od dotychczas proponowanych rozwiązań opartych na interferowaniu i pomiarze wielu wiązek światła za pomocą macierzy detektorów pojedynczych fotonów.

[**Korzystne przykłady wykonania wynalazku**]

Wynalazek zostanie teraz bliżej przedstawiony w przykładach wykonania, z odniesieniem do załączonego rysunku, gdzie na figurach rysunku, linie kropkowane łączące poszczególne elementy układu oznaczają połączenia optyczne (np. światłowód, falowód lub wiązka optyczna w wolnej przestrzeni), natomiast linie ciągłe łączące poszczególne elementy układu oznaczają połączenia elektryczne, na którym ujawniono:

Fig. 1 przedstawia przykład wykonania urządzenia do kwantowego generowania liczb losowych, w którym modulator wielostanowy 150 zrealizowano jako parę dwustanowych modulatorów polaryzacji 251, 252 sterowanych za pomocą układu sterującego 160, gdzie źródło światła 100 generuje koherentną wiązkę optyczną o ustalonej polaryzacji zgodnej lub prostopadłej do kierunku polaryzacji transmitowanego przez element separujący polaryzacje 110, która jest następnie obracana przez parę dwustanowych modulatorów polaryzacji 251, 252. Wiązka optyczna pada na element separujący polaryzacje 110, którego wyjścia 111, 112 monitorowane są przez dwa detektory pojedynczych fotonów 131, 132, połączone elektrycznie 141, 142 z modułem generującym 140.

Fig. 2 przedstawia przykład wykonania urządzenia do kwantowego generowania liczb losowych, w którym modulator wielostanowy 150 zrealizowano jako parę dwustanowych modulatorów polaryzacji 351, 352 sterowanych za pomocą układu sterującego 160, gdzie źródło światła 100 generuje koherentną wiązkę optyczną o ustalonej polaryzacji zgodnej lub prostopadłej do kierunku polaryzacji transmitowanego przez element separujący polaryzacje 110, która jest następnie obracana przez parę dwustanowych modulatorów polaryzacji 351, 352. Wiązka optyczna pada na element separujący polaryzacje 110, którego wyjścia 111, 112 monitorowane są przez dwa detektory pojedynczych fotonów 131, 132, połączone elektrycznie 141, 142 z modułem generującym 140.

Fig. 3 przedstawia przykład wykonania urządzenia do kwantowego generowania liczb losowych wykorzystującego wielostanowy modulator polaryzacji 150 sterowany za pomocą układu sterującego 160, gdzie źródło światła 100 generuje koherentną wiązkę optyczną o ustalonej polaryzacji zgodnej lub prostopadłej do kierunku polaryzacji transmitowanego przez element separujący polaryzacje 110, która jest następnie obracana przez wielostanowy modulator polaryzacji 150. Wiązka optyczna pada na element separujący polaryzacje 110, którego wyjścia 111, 112 monitorowane są przez dwa detektory pojedynczych fotonów 131, 132, połączone elektrycznie 141, 142 z modułem generującym 140.

Fig. 4 przedstawia czworościan (w dwóch różnych rzutach), w trójwymiarowym układzie współrzędnych kartezjańskich, którego osie (μ, λ, f) oznaczają wartości parametrów

modelu fizycznego, wewnątrz czworościanu maksymalne prawdopodobieństwo odgadnięcia losowego bitu przez stronę nieuprawnioną P_g jest mniejsze niż 75%, a tym samym urządzenie pozwala na generowanie prywatnych losowych bitów.

Na figurach rysunku użyto oznaczeń zgodnych z definicjami ze słownika. W stanie techniki znane są różne rodzaje połączeń optycznych i fotonicznych np. światłowód, falowód lub wiązka optyczna w wolnej przestrzeni, które oznaczono na figurach rysunku linią kropkowaną. Linią ciągłą oznaczono na rysunku połączenia elektryczne obejmujące połączenia przewodowe oraz doprowadzenia sygnałów cyfrowych.

[Przykłady wykonania wynalazku]

Poniższe przykłady wykonania wynalazku zostały umieszczone jedynie w celu zilustrowania wynalazku oraz wyjaśnienia poszczególnych jego aspektów, a nie w celu jego ograniczenia i nie powinny być utożsamiane z całym jego zakresem, który zdefiniowano w załączonych zastrzeżeniach patentowych. W poniższych przykładach, jeśli nie wskazano inaczej, stosowano standardowe materiały i metody wykorzystywane w dziedzinie techniki lub postępowano zgodnie z zaleceniami producentów dla określonych urządzeń, materiałów i metod.

PRZYKŁAD 1

Urządzenie do kwantowego generowania liczb losowych wykorzystujące parę dwustanowych modulatorów polaryzacji oraz sposób weryfikacji prywatności sekwencji liczb losowych generowanych za pomocą urządzenia

W poniższym przykładzie przedstawionym na rysunku Fig. 1 źródłem światła 100 o ustalonej polaryzacji jest dioda laserowa emitująca koherentną wiązkę optyczną o polaryzacji pionowej (alternatywnie poziomej). Polaryzacja wiązki jest następnie obracana przez wielostanowy modulator polaryzacji 150 zrealizowany jako para dwustanowych modulatorów polaryzacji oznaczonych na rysunku Fig. 1 jako 251, 252. Na każdy ż modulatorów polaryzacji 251, 252 podawany jest niezależnie cyfrowy sygnał sterujący z układu sterującego 160. Dla każdego z modulatorów, w przypadku gdy na wejście elektryczne modulatora podawana jest wartość bitu sterującego *1*, obraca on polaryzację wiązki optycznej o kąt 45°. Natomiast, w przypadku gdy na wejście elektryczne modulatora podawana jest wartość bitu sterującego *0*, obraca on polaryzację wiązki optycznej o kąt 0°. Działanie modulatora pierwszego 251 nie zależy od działania modulatora drugiego 252. Następnie wiązka optyczna kierowana jest na element separujący polaryzacje 110, korzystnie kostkę dzielącą polaryzację (PBS) ze względu na niską cenę i powszechną dostępność, w której światło spolaryzowane pionowo jest transmitowane, zaś światło spolaryzowane poziomo jest odbijane. Dla polaryzacji ukośnej (obróconej o 45°), kostka dzieląca polaryzacje działa jak zbalansowana płytka światłodzieląca tzn. dzieli wiązkę przychodzącą na dwie wiązki o równej energii. Każda z wyjściowych wiązek kostki dzielącej polaryzacje 111, 112 mierzona jest za pomocą detektora pojedynczych fotonów 131, 132, korzystnie fotodiody lawinowej, lub korzystnie detektora pojedynczych fotonów opartego na nadprzewodnictwie, który cechuje się niezwykle niską liczbą ciemnych zliczeń oraz bardzo wysoką wydajnością kwantową pozwalającą na efektywną detekcję fotonów.

Prawdopodobieństwo kliknięcia w każdym z detektorów może być oznaczone przez P^{I}_{xy} oraz P^{II}_{xy}, gdzie *x* oznacza wartość bitu sterującego podawanego na pierwszy modulator polaryzacji 251, zaś *y* wartość bitu sterującego podawanego na drugi modulator polaryzacji 252. Cyfra rzymska w indeksie górnym oznacza drogę optyczną za kostką PBS, w której umieszczono detektor zgodnie z oznaczeniami na rysunku Fig. 1, gdzie droga optyczna I jest oznaczona jako 111 zaś droga optyczna II jako 112. Dla kombinacji bitów sterujących $\{x, y\} = \{0,1\}$ oraz $\{x,y\} = \{1,0\}$ wiązka padająca na element separujący polaryzacje 110 ma polaryzację ukośną, a w związku z tym zgodnie z regułami optyki kwantowej prawdopodobieństwo kliknięcia detektora umieszczonego w pierwszej drodze optycznej 111 jest takie samo jak prawdopodobieństwo kliknięcia detektora umieszczonego w drugiej drodze optycznej 112 tj. $P^{I}_{10} = P^{II}_{10} = P^{I}_{01} = P^{II}_{01}$. Ustawienie modulatorów polaryzacji $\{x,y\} = \{0,1\}$ oraz $\{x,y\} = \{1,0\}$ pozwala na generację prawdziwie losowego ciągu bitów, w którym wartość bitu *0* odpowiada kliknięciu detektora umieszczonego w drodze optycznej I 111, zaś wartość bitu *1* odpowiada kliknięciu detektora umieszczonego w drodze optycznej II 112. Zliczenia detektorów są analizowane i zamieniane w losową sekwencję bitów przy, pomocy modułu generującego 140.

W celu weryfikacji prywatności generowanej losowej sekwencji na podstawie pomiarów impulsów optycznych wyznaczane są prawdopodobieństwa kliknięć P^{I}_{xy} oraz P^{II}_{xy}, dla trzech kierunków polaryzacji wiązki padającej na element dzielący polaryzacje (polaryzacji pionowej, polaryzacji ukośnej i polaryzacji

poziomej) tj. prawdopodobieństwa P^{I}_{00}, P^{II}_{00} (mierzone przy ustawieniach modulatorów *{x,y} = {0,0}*), prawdopodobieństwa P^{I}_{01}, P^{II}_{01} lub alternatywnie P^{I}_{10}, P^{II}_{10} (mierzone odpowiednio przy ustawieniach modulatorów *{x,y} = {0,1}* fub *alternatywnie {x,y} = {1,0})* oraz prawdopodobieństwa P^{I}_{11}, P^{II}_{11} (mierzone przy ustawieniach modulatorów *{x,y} = {1,1}).* Podczas tej procedury testującej urządzenie nie pozwala na generację liczb losowych. W wyidealizowanym scenariuszu wartości prawdopodobieństw dla ustawień *{x,y} = {0,0}* wynoszą odpowiednio $P^{I}_{00} = 1$ oraz $P^{II}_{00} = 0$, dla ustawień *{x,y} = {1,1}* odpowiednio $P^{I}_{11} = 0$ oraz $P^{II}_{11} = 1$, zaś dla ustawień, *{x,y} = {1,0}* oraz *{x,y) = {0,1}* odpowiednio $P^{I}_{10} = P^{II}_{10} = P^{I}_{01} = P^{II}_{01} = 50\%$. Ze względu na ciemne zliczenia detektorów, skończony współczynnik ekstynkcji elementu separującego polaryzacje, lub potencjalną ingerencję strony nieuprawnionej, zmierzone prawdopodobieństwa odbiegać będą od tych z wyidealizowanego scenariusza. Na podstawie zmierzonych wartości $P^{I}_{00}, P^{II}_{00}, P^{I}_{11}, P^{II}_{11}, P^{I}_{01}, P^{II}_{01}$ lub alternatywnie $P^{I}_{00}, P^{II}_{00}, P^{I}_{11}, P^{II}_{11}, P^{I}_{10}, P^{II}_{10}$ oraz wykorzystując rachunek prawdopodobieństwa i model fizyczny układu optycznego można obliczyć zestaw następujących parametrów modelu fizycznego układu generatora:

- μ – średnia liczba fotonów w impulsie światła laserowego mierzonego przy użyciu detektorów, którego pomiar pozwala na generację losowego bitu;
- λ – współczynnik transmisji, gdzie $\lambda = cos^2(\gamma)$, gdzie γ oznacza kąt obrotu polaryzacji wiązki optycznej padającej na element separujący polaryzacje. Podczas procedury testującej zakłada się, że kąt ten może odbiegać od wartości wynikającej z wartości bitów sterujących modulatorami polaryzacji ze względu na ingerencję strony nieuprawnionej. W szczególności zakłada się, że podczas ustawień modulatorów *{x,y} = {1,0}* oraz *{x,y} = (0,1},* kąt γ może być inny niż 45°;
- prawdopodobieństwo *f* przy ustawieniu modulatorów polaryzacji *{x,y} = {0,0}* oznacza prawdopodobieństwo, że ze względu na ingerencję strony nieuprawnionej detektor 131 umieszczony w drodze optycznej I pomimo, zaobserwowania fotonu, nie wysłał do modułu generującego impulsu elektrycznego, z kolei przy ustawieniu modulatorów polaryzacji *{x,y} = {1,1}* prawdopodobieństwo, *f* oznacza prawdopodobieństwo, że ze względu na ingerencję strony nieuprawnionej detektor 132 umieszczony w, drodze optycznej II pomimo, zaobserwowania fotonu nie wysłał do modułu generującego 140 impulsu elektrycznego.

Na podstawie wyznaczonych wartości powyższych parametrów modelu fizycznego *(μ_0, λ_0, f_0)* określane jest maksymalne prawdopodobieństwo odgadnięcia losowego bitu przez stronę nieuprawnioną P_g. Jeśli maksymalne prawdopodobieństwo P_g spełnia nierówność $P_g < X$, gdzie X to maksymalna akceptowalna wartość prawdopodobieństwa odgadnięcia losowego bitu przez stronę nieuprawnioną przyjmująca wartości od 50% do 100%, urządzenie jest zdolne do generowania losowych bitów prywatnych. Korzystnie, maksymalne prawdopodobieństwo odgadnięcia losowego bitu przez stronę nieuprawnioną P_g powinno być mniejsze niż 75%. Warunek $P_g < 75\%$ jest spełniony gdy punkt *(μ_0, λ_0, f_0)* w przestrzeni trójwymiarowej *(μ, λ, f)* zdefiniowany przez wyznaczone wartości parametrów modelu fizycznego, znajduje się wewnątrz czworościanu, przedstawionego na Fig. 4, którego wierzchołki znajdują się w punktach;

- *(μ=0, λ=0, f=0);*
- *(μ=0, λ=0,75, f=0);*
- *(μ=10, λ=0, f=0);*
- *(μ=0, λ=0, f=0).*

Dla strategii strony nieuprawnionej polegającej na odgadywaniu losowych bitów bez żadnej dodatkowej informacji maksymalne prawdopodobieństwo P_g wynosi 50%.

PRZYKŁAD 2

Alternatywne urządzenie do kwantowego generowania liczb losowych wykorzystujące parę dwustanowych modulatorów polaryzacji oraz sposób weryfikacji prywatności sekwencji liczb losowych generowanych za pomocą urządzenia

W poniższym przykładzie przedstawionym na rysunku Fig. 2 źródłem światła 100 o ustalonej polaryzacji jest dioda laserowa emitująca koherentną wiązkę optyczną o polaryzacji pionowej (alternatywnie poziomej). Polaryzacja wiązki jest następnie obracana, przez wielostanowy modulator polaryzacji 150 zrealizowany jako para dwustanowych modulatorów polaryzacji oznaczonych na rysunku Fig. 2

jako 351, 352. Na każdy z modulatorów polaryzacji 351, 352 podawany jest niezależnie cyfrowy sygnał sterujący z układu sterującego 160. Dla pierwszego z modulatorów 351 w przypadku gdy na wejście elektryczne modulatora podawana jest wartość bitu sterującego *0*, obraca on polaryzację wiązki optycznej o kąt 0°, natomiast w przypadku gdy na wejście elektryczne modulatora podawana jest wartość bitu sterującego *1*, obraca on polaryzację wiązki optycznej o kąt 45°. Dla drugiego z modulatorów 352, w przypadku gdy na wejście elektryczne modulatora podawana; jest wartość bitu sterującego 0, obraca on polaryzację wiązki optycznej o kąt 0°, natomiast w przypadku gdy na wejście elektryczne modulatora podawana jest wartość bitu sterującego *1*, obraca on polaryzację wiązki optycznej o kąt 90°. Działanie modulatora pierwszego 351 nie zależy od działania modulatora drugiego 352. Kolejność modulatorów 351 oraz 352 w torze optycznym nie wpływa na działanie urządzenia. W tym przykładzie modulator 351 obracający wiązkę o 45° umieszczony jest w torze optycznym bliżej źródła światła 100 niż drugi modulator 352 obracający wiązkę o 90°. Następnie wiązka optyczna kierowana jest na element separujący polaryzacje 110, korzystnie kostkę dzielącą polaryzację (PBS) ze względu na niską cenę i powszechną dostępność, w której światło spolaryzowane pionowo jest transmitowane, zaś światło spolaryzowane poziomo jest odbijane. Dla polaryzacji ukośnej (obróconej o 45° lub 135°), kostka dzieląca polaryzacje działa jak zbalansowana płytka światłodzieląca tzn. dzieli wiązkę przychodzącą na dwie wiązki o równej energii. Każda z wyjściowych wiązek kostki dzielącej polaryzacje 111, 112 mierzona jest za pomocą detektora pojedynczych fotonów 131, 132, korzystnie fotodiody lawinowej, lub korzystnie detektora pojedynczych fotonów opartego na nadprzewodnictwie, który cechuje się niezwykle niską liczbą ciemnych zliczeń oraz bardzo wysoką wydajnością kwantową pozwalającą na efektywną detekcję fotonów.

Prawdopodobieństwo kliknięcia w każdym z detektorów może być oznaczone przez P^{I}_{xy} oraz P^{II}_{xy}, gdzie *x* oznacza wartość bitu sterującego podawanego na pierwszy modulator polaryzacji 351, zaś *y* wartość bitu sterującego podawanego na drugi modulator polaryzacji 352. Cyfra rzymska w indeksie górnym oznacza drogę optyczną za kostką PBS, w której umieszczono detektor zgodnie z oznaczeniami na rysunku Fig. 2, gdzie droga optyczna I jest oznaczona jako 111 zaś droga optyczna II jako 112. Dla kombinacji bitów sterujących *{xy} = {1,0} lub {xy} = {1,1}* wiązka padająca na element separujący polaryzacje 110 ma polaryzację ukośną, a w związku z tym zgodnie z regułami optyki kwantowej prawdopodobieństwo kliknięcia detektora umieszczonego w pierwszej drodze optycznej 111, jest takie samo jak prawdopodobieństwo kliknięcia detektora umieszczonego w drugiej drodze optycznej 112 tj. $P^{I}_{10} = P^{II}_{10} = P^{I}_{11} = P^{II}_{11}$. Ustawienie modulatorów polaryzacji *{x,y} = {1,0}* lub *{x,y} = {1,1}* pozwala więc na generację prawdziwie losowego ciągu bitów, w którym wartość bitu *0* odpowiada kliknięciu detektora umieszczonego w drodze optycznej I 111, zaś wartość bitu *1* odpowiada kliknięciu detektora umieszczonego w drodze optycznej II 112. Zliczenia detektorów są analizowane i zamieniane w losową sekwencję bitów przy pomocy modułu generującego 140.

W celu weryfikacji prywatności generowanej losowej sekwencji na podstawie pomiarów impulsów optycznych wyznaczane są prawdopodobieństwa kliknięć P^{I}_{xy} oraz P^{II}_{xy}, dla trzech kierunków polaryzacji wiązki padającej, na element dzielący polaryzacje, (polaryzacji, pionowej, polaryzacji ukośnej i polaryzacji poziomej) tj. prawdopodobieństwa P^{I}_{00}, P^{II}_{00} (mierzone przy ustawieniach modulatorów *{x,y}= {0,0})*, prawdopodobieństwa P^{I}_{10}, P^{II}_{10}, lub alternatywnie P^{I}_{11}, P^{II}_{11}, (mierzone przy ustawieniach modulatorów *{x,y} = {1,0}* lub alternatywnie *{x,y} = {1,1})* oraz prawdopodobieństwa P^{I}_{01}, P^{II}_{01}, (mierzone przy ustawieniach modulatorów *{x,y} = (0,1}).* Podczas tej procedury testującej urządzenie nie pozwala na generację liczb losowych. W wyidealizowanym scenariuszu wartości prawdopodobieństw dla ustawień *{x,y} = {0,0}* wynoszą odpowiednio $P^{I}_{00} = 1$ oraz $P^{II}_{00} = 0$, dla ustawień *{x,y} = {0,1}* odpowiednio $P^{I}_{01} = 0$ oraz $P^{II}_{01} = 1$, zaś dla ustawień *{x,y} = {1,0}* oraz *{x,y} = {1,1}* odpowiednio $P^{I}_{10} = P^{II}_{10} = P^{I}_{11} = P^{II}_{11} = 50\%$. Ze względu na. ciemne zliczenia detektorów, skończony współczynnik ekstynkcji elementu separującego polaryzacje, lub potencjalną ingerencję strony nieuprawnionej, zmierzone prawdopodobieństwa odbiegać będą od tych z wyidealizowanego scenariusza. Na podstawie zmierzonych wartości $P^{I}_{00}, P^{II}_{00}, P^{I}_{01}, P^{II}_{01}, P^{I}_{10}, P^{II}_{10}$ lub alternatywnie $P^{I}_{00}, P^{II}_{00}, P^{I}_{01}, P^{II}_{01}, P^{I}_{11}, P^{II}_{11}$ oraz wykorzystując rachunek prawdopodobieństwa i model fizyczny układu optycznego można obliczyć zestaw następujących parametrów modelu fizycznego układu generatora:

- μ – średnia liczba fotonów w impulsie światła laserowego mierzonego przy użyciu detektorów, którego pomiar pozwala na generację losowego bitu;
- λ – współczynnik transmisji, gdzie $\lambda = cos^2(y)$, gdzie y oznacza kąt obrotu polaryzacji wiązki optycznej padającej na element separujący polaryzacje. Podczas procedury, testującej zakłada się, że kąt ten może odbiegać od wartości wynikającej z wartości bitów sterujących modulatorami polaryzacji ze względu na ingerencję strony nieuprawnionej. W szczególności zakłada się, że podczas ustawień modulatorów *{xy} = {1,0}* oraz *{x,y} = {1,1},* kąt γ może być inny niż 45° lub 135°;
- prawdopodobieństwo *f* – przy ustawieniu modulatorów polaryzacji *{x,y} = {0,0}* oznacza prawdopodobieństwo, że ze względu na ingerencję strony nieuprawnionej detektor 131 umieszczony w drodze optycznej I pomimo zaobserwowania fotonu nie wysłał do modułu generującego, impulsu elektrycznego, z kolei przy ustawieniu modulatorów polaryzacji *{x,y} = {0,1}* prawdopodobieństwo *f* oznacza prawdopodobieństwo, że ze względu na ingerencję strony nieuprawnionej detektor 132 umieszczony w drodze optycznej II pomimo zaobserwowania fotonu nie wysłał do modułu generującego 140 impulsu elektrycznego.

Na podstawie wyznaczonych wartości powyższych parametrów modelu fizycznego *(μ_0, λ_0, f_0)* określane jest maksymalne prawdopodobieństwo odgadnięcia losowego bitu przez stronę nieuprawnioną P_g. Jeśli maksymalne prawdopodobieństwo P_g spełnia nierówność $P_g < X$, gdzie X to maksymalna akceptowalna wartość prawdopodobieństwa odgadnięcia losowego bitu przez stronę nieuprawnioną przyjmująca wartości od 50% do 100%, urządzenie jest zdolne do generowania losowych bitów prywatnych. Korzystnie, maksymalne prawdopodobieństwo odgadnięcia losowego bitu przez stronę nieuprawnioną P_g powinno być mniejsze niż 75%. Warunek $P_g < 75\%$ jest spełniony gdy punkt *(μ_0, λ_0, f_0)* w przestrzeni trójwymiarowej *(μ, λ, f)* zdefiniowany przez wyznaczone wartości parametrów modelu fizycznego, znajduje się wewnątrz czworościanu, przedstawionego na Fig. 4, którego wierzchołki znajdują się w punktach:

- *(μ=0, λ=0, f=0);*
- *(μ=0, λ=0,75, f=0);*
- *(μ=10, λ=0, f=0);*
- *(μ=0, λ=0, f=1).*

Dla strategii strony nieuprawnionej polegającej na odgadywaniu losowych bitów bez żadnej dodatkowej informacji maksymalne prawdopodobieństwo P_g wynosi 50%.

PRZYKŁAD 3

Urządzenie do kwantowego generowania liczb losowych wykorzystujące wielostanowy modulator polaryzacji oraz sposób weryfikacji prywatności sekwencji liczb losowych generowanych za pomocą urządzenia

W poniższym przykładzie przedstawionym na rysunku Fig. 3 źródłem światła 100 o ustalonej polaryzacji jest dioda laserowa emitująca koherentną wiązkę optyczną o polaryzacji pionowej (alternatywnie poziomej). Polaryzacja wiązki jest następnie obracana, przez pojedynczy wielostanowy modulator polaryzacji oznaczony na rysunku Fig. 3 jako 150. Na modulator podawany jest analogowy sygnał sterujący z układu sterującego 160. W przypadku gdy na wejście elektryczne modulatora podawane jest napięcie V_0 obraca on polaryzację wiązki optycznej o kąt 0°, w przypadku gdy na wejście elektryczne modulatora podawane jest napięcie V_1 obraca on polaryzację wiązki optycznej o kąt γ = 45°, w przypadku gdy na wejście elektryczne modulatora podawane jest napięcie V_2 obraca on polaryzację wiązki optycznej o kąt 2γ = 90°. Następnie wiązka optyczna kierowana jest na element separujący polaryzacje 110, korzystnie kostkę dzielącą polaryzację (PBS) ze względu na niską cenę i powszechną dostępność, w której światło spolaryzowane pionowo jest transmitowane, zaś światło spolaryzowane poziomo jest odbijane. Dla polaryzacji ukośnej (obróconej o 45°), kostka dzieląca polaryzacje działa jak zbalansowana płytka światłodzieląca tzn. dzieli wiązkę przychodzącą na dwie wiązki o równej energii. Każda z wyjściowych wiązek kostki dzielącej polaryzacje 111, 112 mierzona jest za pomocą detektora pojedynczych fotonów 131, 132, korzystnie fotodiody lawinowej, lub korzystnie detektora pojedynczych fotonów opartego na nadprzewodnictwie, który cechuje się niezwykle niską liczbą ciemnych zliczeń oraz bardzo wysoką wydajnością kwantową pozwalającą na efektywną detekcję fotonów.

Prawdopodobieństwo kliknięcia w każdym z detektorów może być oznaczone przez p_v^I oraz p_v^{II}, gdzie v oznacza wartość napięcia podawanego na wejście elektryczne modulatora polaryzacji 150. Cyfra rzymska w indeksie górnym oznacza drogę optyczną za kostką PBS, w której

umieszczono detektor zgodnie z oznaczeniami na rysunku Fig. 1, gdzie droga optyczna I jest oznaczona jako 111, zaś droga optyczna II jako 112. Dla napięcia sterującego V_1 wiązka padająca na element separujący polaryzacje 110 ma polaryzację ukośną, a w związku z tym zgodnie z regułami optyki kwantowej prawdopodobieństwo kliknięcia detektora umieszczonego w pierwszej drodze optycznej 111 jest takie samo jak prawdopodobieństwo kliknięcia detektora umieszczonego w drugiej drodze optycznej 112 tj. $P^{I}_{V_1} = P^{II}_{V_1}$. Napięcie podawane na wejście elektryczne modulatora polaryzacji $v = V_1$ pozwala więc na generację prawdziwie losowego ciągu bitów, w którym wartość bitu *0* odpowiada kliknięciu detektora umieszczonego w drodze optycznej I 111, zaś wartość bitu *1* odpowiada kliknięciu detektora umieszczonego w drodze optycznej II 112. Zliczenia detektorów są analizowane i zamieniane w losową sekwencję bitów przy pomocy modułu generującego 140.

W celu weryfikacji prywatności generowanej losowej sekwencji na podstawie pomiarów impulsów optycznych wyznaczane są prawdopodobieństwa kliknięć P^{I}_{v} oraz P^{II}_{v}, dla trzech kierunków polaryzacji wiązki padającej na element dzielący polaryzacje (polaryzacji pionowej, polaryzacji ukośnej i polaryzacji poziomej) tj. prawdopodobieństwa $P^{I}_{V_0}$, $P^{II}_{V_0}$ (mierzone przy podanym na wejście elektryczne modulatora napięciu V_0), prawdopodobieństwa $P^{I}_{V_1}$, $P^{II}_{V_1}$ (mierzone przy podanym na wejście elektryczne modulatora napięciu V_1) oraz prawdopodobieństwa $P^{I}_{V_2}$, $P^{II}_{V_2}$ (mierzone przy podanym na wejście elektryczne modulatora napięciu V_2). Podczas tej procedury testującej urządzenie nie pozwala na generację liczb losowych. W wyidealizowanym scenariuszu wartości prawdopodobieństw dla napięcia podawanego na wejście modulatora $v = V_0$ wynoszą odpowiednio $P^{I}_{V_0} = 1$ oraz $P^{II}_{V_0} = 0$, dla napięcia podawanego na wejście modulatora $v = V_2$ odpowiednio $P^{I}_{V_2} = 0$ oraz $P^{II}_{V_2} = 1$, zaś dla napięcia podawanego na wejście modulatora $v = V_1$ odpowiednio $P^{I}_{V_1} = P^{II}_{V_1} = 50\%$. Ze względu na ciemne zliczenia detektorów, skończony współczynnik ekstynkcji elementu separującego polaryzacje, lub potencjalną ingerencję strony nieuprawnionej, zmierzone prawdopodobieństwa odbiegać będą od tych z wyidealizowanego scenariusza. Na podstawie zmierzonych wartości $P^{I}_{V_0}, P^{II}_{V_0}, P^{I}_{V_1}, P^{II}_{V_1}, P^{I}_{V_2}, P^{II}_{V_2}$ wykorzystując rachunek prawdopodobieństwa i model fizyczny układu optycznego można obliczyć zestaw następujących parametrów modelu fizycznego układu generatora:

- μ – średnia liczba fotonów w impulsie światła laserowego mierzonego przy użyciu detektorów, którego pomiar pozwala na generację losowego bitu;
- λ – współczynnik transmisji, gdzie $\lambda = cos^2(\gamma)$, gdzie γ oznacza kąt obrotu polaryzacji wiązki optycznej padającej na element separujący polaryzacje. Podczas procedury testującej zakłada się, że kąt ten może odbiegać od wartości wynikającej z wartości napięcia podawanego na wejście elektryczne modulatora ze względu na ingerencję strony nieuprawnionej. W szczególności zakłada się, że dla napięcia podawanego na wejście elektryczne modulatora $v = V_1$ kąt γ może być inny niż 45° oraz dla napięcia podawanego na wejście modulatora $v = V_2$ *kąt* 2γ może być inny niż 90°;
- prawdopodobieństwo *f* przy napięciu podawanym na wejście elektryczne modulatora polaryzacji $v = V_0$, oznacza prawdopodobieństwo, że ze względu na ingerencję strony nieuprawnionej detektor 131 umieszczony w drodze optycznej I pomimo zaobserwowania fotonu nie wysłał do układu elektronicznego impulsu elektrycznego, z kolei przy napięciu podawanym na wejście elektryczne modulatora polaryzacji w generatorze $v = V_2$, prawdopodobieństwo *f* oznacza prawdopodobieństwo, że ze względu na ingerencję strony nieuprawnionej detektor 132 umieszczony w drodze optycznej II pomimo zaobserwowania fotonu nie wysłał do modułu generującego 140 impulsu elektrycznego.

Na podstawie wyznaczonych wartości powyższych parametrów modelu fizycznego (μ_0, λ_0, f_0) określane jest maksymalne prawdopodobieństwo odgadnięcia losowego bitu przez stronę nieuprawnioną P_g. Jeśli maksymalne prawdopodobieństwo P_g spełnia nierówność $P_g < X$, gdzie X to maksymalna akceptowalna wartość prawdopodobieństwa odgadnięcia losowego bitu przez stronę nieuprawnioną przyjmująca wartości od 50% do 100%, urządzenie jest zdolne do generowania losowych bitów prywatnych. Korzystnie, maksymalne prawdopodobieństwo odgadnięcia losowego bitu przez stronę nieuprawnioną P_g powinno być mniejsze niż 75%. Warunek $P_g < 75\%$ jest spełniony gdy punkt (μ_0, λ_0, f_0) w prze-

strzeni trójwymiarowej *(μ, λ, f)* zdefiniowany przez wyznaczone wartości parametrów modelu fizycznego, znajduje się wewnątrz czworościanu, przedstawionego na Fig. 4, którego wierzchołki znajdują się w punktach:

- *(μ=0, λ=0, f=0);*
- *(μ=0, λ=0,75, f=0);*
- *(μ=10, λ=0, f=0);*
- *(μ=0, λ=0, f=1).*

Dla strategii strony nieuprawnionej polegającej na odgadywaniu losowych bitów bez żadnej dodatkowej informacji maksymalne prawdopodobieństwo wynosi 50%.

[Możliwe obszary wykorzystania wynalazku]

Niniejszy wynalazek znajduje zastosowanie m.in. w obszarach techniki: cyberbezpieczeństwa informatycznego i teleinformatycznego, szyfrowaniu danych oraz kryptografii. Generatory liczb losowych są powszechnie używane wśród użytkowników sieci komputerowych i telefonicznych. Ponadto ich zastosowania są szczególnie ważne podczas szyfrowania danych wrażliwych w sektorze bankowo-finansowym, energetyce, sterowaniu i automatyce przemysłowej, przy zabezpieczeniu wrażliwych danych medycznych, w sektorze militarnym, podczas komunikacji w administracji rządowej oraz w służbach specjalnych i korpusie dyplomatycznym (gdzie nadawanie i odbieranie komunikatów z odległych placówek jest narażone na podsłuch przez osoby niepowołane).

Ponadto wynalazek znajduje zastosowanie w grach losowych, ze szczególnym uwzględnieniem gier liczbowych, których zasady opierają się na prawdziwej losowości zdarzeń uniemożliwiającej przewidzenie wyniku losowania przez osoby trzecie. Generatory liczb losowych znajdują również zastosowania w symulacjach numerycznych, które wymagają prawdziwie losowego próbkowania np. metoda Monte Carlo.

Zastrzeżenia patentowe

1. Urządzenie do kwantowej generacji liczb losowych zawierające źródło światła (100) o ustalonej polaryzacji oraz połączony z nim torem optycznym element dzielący polaryzacje (110) mający pierwsze wyjście (111) odpowiadające polaryzacji pionowej i drugie wyjście (112) odpowiadające polaryzacji poziomej oraz pierwszy detektor (131) połączony torem optycznym z pierwszym wyjściem (111) elementu dzielącego polaryzacje (110) i drugi detektor (132) połączony torem optycznym z drugim wyjściem (112) elementu dzielącego polaryzacje (110), moduł generujący (140), mający pierwsze wejście (141) połączone z wyjściem pierwszego detektora (131) oraz drugie wejście (142) połączone z wyjściem drugiego detektora (132), oraz wyjście dwustanowe (143), przystosowany do generowania, na wyjściu dwustanowym (143) bitów o wartości *1* po otrzymaniu sygnału na pierwszym wejściu (141) i bitów o wartości *0* po otrzymaniu sygnału na drugim wejściu (142), **znamienne tym**, że źródło światła (100) jest połączone z elementem dzielącym polaryzacje (110) za pośrednictwem wielostanowego modulatora polaryzacji (150) sterowanego sygnałem cyfrowym lub analogowym generowanym za pomocą elektronicznego układu sterującego (160) połączonego z wielostanowym modulatorem polaryzacji (150).
2. Urządzenie według zastrz. 1 **znamienne tym**, że wielostanowy modulator polaryzacji (150), zawiera dwa połączone ze sobą torem optycznym dwustanowe modulatory polaryzacji (251) oraz (252) przy czym oba modulatory przystosowane są do obrotu polaryzacji o 45° gdy na ich wejście elektryczne podawany jest sterujący sygnał cyfrowy o wartości bitu *1* oraz do obrotu polaryzacji o 0° gdy na ich wejście elektryczne podawany jest sterujący sygnał cyfrowy o wartości bitu *0*, lub alternatywnie do obrotu polaryzacji o 45° gdy na ich wejście elektryczne podawany jest sterujący sygnał cyfrowy o wartości bitu *0* oraz do obrotu polaryzacji o 0° gdy na ich wejście elektryczne podawany jest sterujący sygnał cyfrowy o wartości bitu *1*.
3. Urządzenie według zastrz. 1 **znamienne tym**, że wielostanowy modulator polaryzacji (150), zawiera dwa połączone ze sobą torem optycznym dwustanowe modulatory polaryzacji (351) oraz (352), przy czym jeden z modulatorów (351, 352) obraca polaryzację o 45° gdy na jego wejście elektryczne podawany jest sygnał cyfrowy o wartości bitu *1* oraz obraca polaryzację o 0° gdy na jego wejście elektryczne podawany jest sygnał cyfrowy o wartości bitu *0*, zaś odpowiednio drugi z modulatorów (351, 352) obraca polaryzację o 90° gdy na jego wejście

elektryczne podawany jest sygnał cyfrowy o wartości bitu *1* oraz obraca polaryzację o 0° gdy na jego wejście elektryczne podawany jest sygnał cyfrowy o wartości bitu *0*.

4. Urządzenie według zastrz. 1 **znamienne tym**, że wielostanowy modulator polaryzacji (150), zawiera dwa połączone ze sobą torem optycznym dwustanowe modulatory polaryzacji (351) oraz (352), przy czym jeden z modulatorów (351, 352) obraca polaryzację o 45° gdy na jego wejście elektryczne podawany jest sygnał cyfrowy o wartości bitu *0* oraz obraca polaryzację o 0° gdy na jego wejście elektryczne podawany jest sygnał cyfrowy o wartości bitu *1*, zaś drugi z modulatorów, odpowiednio (351, 352) obraca polaryzację o 90° gdy na jego wejście elektryczne podawany jest sygnał cyfrowy o wartości bitu *0* oraz obraca polaryzację o 0° gdy na jego wejście elektryczne podawany jest sygnał cyfrowy o wartości bitu *1*.
5. Urządzenie według któregokolwiek z zastrz. 1–4 **znamienne tym**, że elementem separującym polaryzacje (110) jest kostka dzieląca polaryzacje z powłoką dielektryczną lub polaryzator oparty na dwójłomności lub pryzmat.
6. Urządzenie według któregokolwiek z zastrz. 1–5 **znamienne tym**, że źródłem światła (100) jest źródło światła koherentnego, korzystnie zawierające diodę laserową lub. laser impulsowy, lub źródło światła niekoherentnego korzystnie zawierające diodę LED, lub źródło pojedynczych fotonów, korzystnie oparte na pojedynczych atomach lub kropkach kwantowych.
7. Urządzenie według któregokolwiek z zastrz. 1–6 **znamienne tym**, że źródło światła (100) jest przystosowane do emitowania impulsów światła o polaryzacji pionowej lub poziomej.
8. Urządzenie według któregokolwiek z zastrz. 1–7 **znamienne tym**, że źródło światła (100) jest przystosowane do generowania wiązki optycznej o centralnej długości fali w zakresie 400–1600 nm, której średnia energia jest mniejsza niż 1 μW.
9. Urządzenie według któregokolwiek z zastrz. 1–8 **znamienne tym**, że oba detektory pojedynczych fotonów (131) i (132) zawierają fotodiodę lawinową lub detektor pojedynczych fotonów oparty na nadprzewodnictwie, lub alternatywnie jeden z detektorów (131, 132) zawiera fotodiodę lawinową, zaś drugi z detektorów zawiera detektor pojedynczych fotonów oparty na nadprzewodnictwie.
10. Urządzenie według któregokolwiek z zastrz. 1–9 **znamienne tym**, że torem optycznym jest światłowód, falowód lub wiązka optyczna w wolnej przestrzeni.
11. Sposób weryfikacji prywatności sekwencji bitów losowych generowanych za pomocą urządzenia do kwantowej generacji liczb losowych zawierającego źródło światła (100) o ustalonej polaryzacji oraz połączony z nim element dzielący polaryzacje (110) mający pierwsze wyjście (111) odpowiadające polaryzacji pionowej i drugie wyjście (112) odpowiadające polaryzacji poziomej, oraz pierwszy detektor (131) połączony z pierwszym wyjściem (111) elementu dzielącego polaryzacje (110) i drugi detektor (132) połączony z drugim wyjściem (112) elementu dzielącego polaryzacje (110), moduł generujący (140), mający pierwsze wejście (141) połączone z wyjściem pierwszego detektora (131) oraz drugie wejście (142) połączone z wyjściem drugiego detektora (132), oraz wyjście dwustanowe (143), przystosowany do generowania na wyjściu dwustanowym (143) bitów o wartości *1* po otrzymaniu sygnału na pierwszym wejściu (141) i bitów o wartości *0* po otrzymaniu sygnału na drugim wejściu (142), w układzie podczas generowania liczb losowych polaryzacja wiązki padającej na element separujący polaryzacje jest ukośna, czyli obrócona o 45° względem kierunku polaryzacji transmitowanego przez element separujący polaryzacje **znamienny tym**, że podczas weryfikacji prywatności za pomocą układu sterowania (160) steruje się wielostanowym modulatorem polaryzacji (150) i obraca się polaryzację światła padającego na element separujący polaryzacje (110), ustawiając ją kolejno pod kątem 0°, 45°, oraz 90° do kierunku polaryzacji transmitowanego przez element separujący polaryzacje oraz dla każdego z trzech kierunków polaryzacji (0°, 45°, 90°) rejestruje się sekwencję bitów generowanych przez moduł generujący (140), a następnie na podstawie każdej z trzech sekwencji wyznacza się prawdopodobieństwo zarejestrowania zliczenia przez pierwszy detektor (131) oraz prawdopodobieństwo zarejestrowania zliczenia przez drugi detektor (132) oraz na podstawie sześciu prawdopodobieństw $(P^{I}_{00}, P^{II}_{00}, P^{I}_{11}, P^{II}_{11}, P^{I}_{01}, P^{II}_{01}$ lub $P^{I}_{00}, P^{II}_{00}, P^{I}_{11}, P^{II}_{11}, P^{I}_{10}, P^{II}_{10}$ lub $P^{I}_{00}, P^{II}_{00}, P^{I}_{01}, P^{II}_{01}, P^{I}_{10}, P^{II}_{10}$ lub $P^{I}_{00}, P^{II}_{00}, P^{I}_{01}, P^{II}_{01}, P^{I}_{11}, P^{II}_{11}$ lub $P^{I}_{V_0}, P^{II}_{V_0}, P^{I}_{V_1}, P^{II}_{V_1}, P^{I}_{V_2}, P^{II}_{V_2})$ oblicza się parametry modelu fizycznego układu, które stosuje się do wyznaczenia maksymalnego prawdopodobieństwa odgadnięcia losowego bitu przez stronę nieuprawnioną P_g i wery-

fikację prywatności uznaje się za pozytywną jeżeli maksymalne prawdopodobieństwo odgadnięcia losowego bitu przez stronę nieuprawnioną P_g jest mniejsze niż maksymalna akceptowalna wartość prawdopodobieństwa odgadnięcia losowego bitu przez stronę nieuprawnioną X, gdy weryfikacja jest pozytywna urządzenie jest zdolne do generowania losowych bitów prywatnych.

12. Sposób według zastrz. 11 **znamienny tym**, że do wyznaczenia maksymalnego prawdopodobieństwa odgadnięcia losowego bitu przez stronę nieuprawnioną P_g stosuje się model fizyczny, którego parametrami są:
    (a) średnia liczba fotonów w mierzonych impulsach – μ;
    (b) współczynnik transmisji – λ;
    (c) prawdopodobieństwo f.
13. Sposób według zastrz. 11 albo 12 **znamienny tym**, że weryfikację prywatności generowanej sekwencji bitów losowych uznaje się za pozytywną w zależności od przynależności wyznaczonych wartości parametrów modelu fizycznego (μ_0, λ_0, f_0) do predefiniowanego zbioru wartości liczbowych w przestrzeni trójwymiarowej (μ, λ, f) wyliczonego na podstawie modelu fizycznego oraz na podstawie maksymalnej akceptowalnej wartości prawdopodobieństwa odgadnięcia losowego bitu przez stronę nieuprawnioną X.
14. Sposób według zastrz. 13 **znamienny tym**, że maksymalna akceptowalna wartość prawdopodobieństwa odgadnięcia losowego bitu przez stronę nieuprawnioną X znajduje się w przedziale od 50% do 100%.
15. Sposób według zastrz. 14 **znamienny tym**, że maksymalna akceptowalna wartość prawdopodobieństwa odgadnięcia losowego bitu przez stronę nieuprawnioną X wynosi 75%, dla $X = 75\%$ weryfikacja prywatności generowanej sekwencji bitów losowych jest pozytywna (tj. $P_g < 75\%$), gdy wyznaczone wartości parametrów, modelu fizycznego (μ_0, λ_0, f_0) znajdują się wewnątrz czworościanu, którego wierzchołki znajdują się w następujących punktach przestrzeni trójwymiarowej (μ, λ, f):
    - $(\mu=0, \lambda=0, f=0)$;
    - $(\mu=0, \lambda=0{,}75, f=0)$;
    - $(\mu=10, \lambda=0, f=0)$;
    - $(\mu=0, \lambda=0, f=1)$.
16. Produkt komputerowy, **znamiennym tym**, że zawiera oprogramowanie, które po wgraniu do układu sterującego (160) i modułu generującego (140) realizuje sposób określony w zastrzeżeniach od 11 do 15.

Rysunki

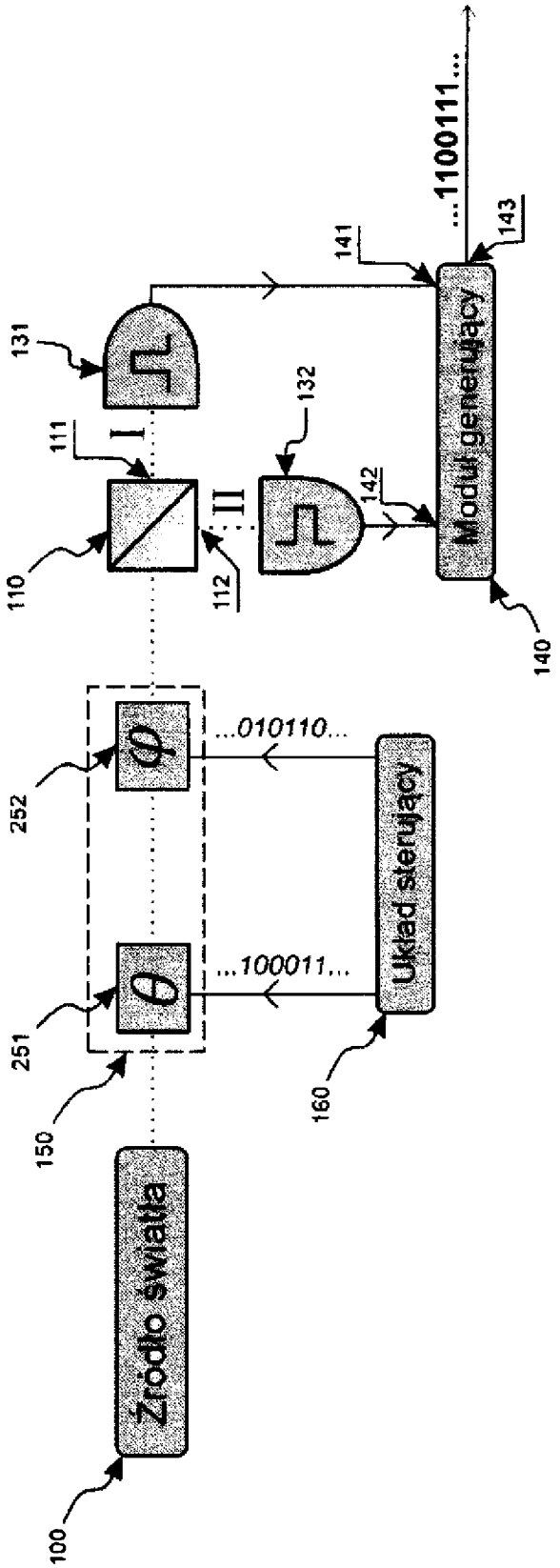

Fig. 1

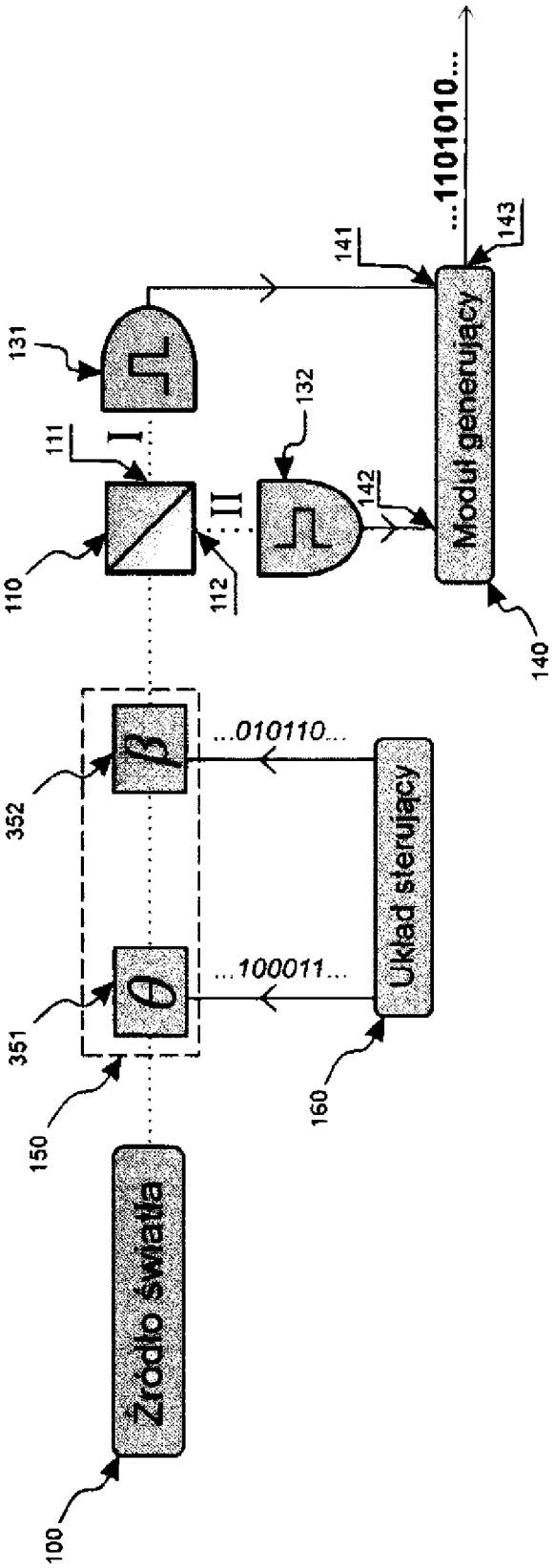
...1101010...
143
141
131
132
111
I
II
142
110
112
Moduł generujący
140
...010110...
352
...100011...
351
Układ sterujący
160
150
Źródło światła
100

Fig. 2

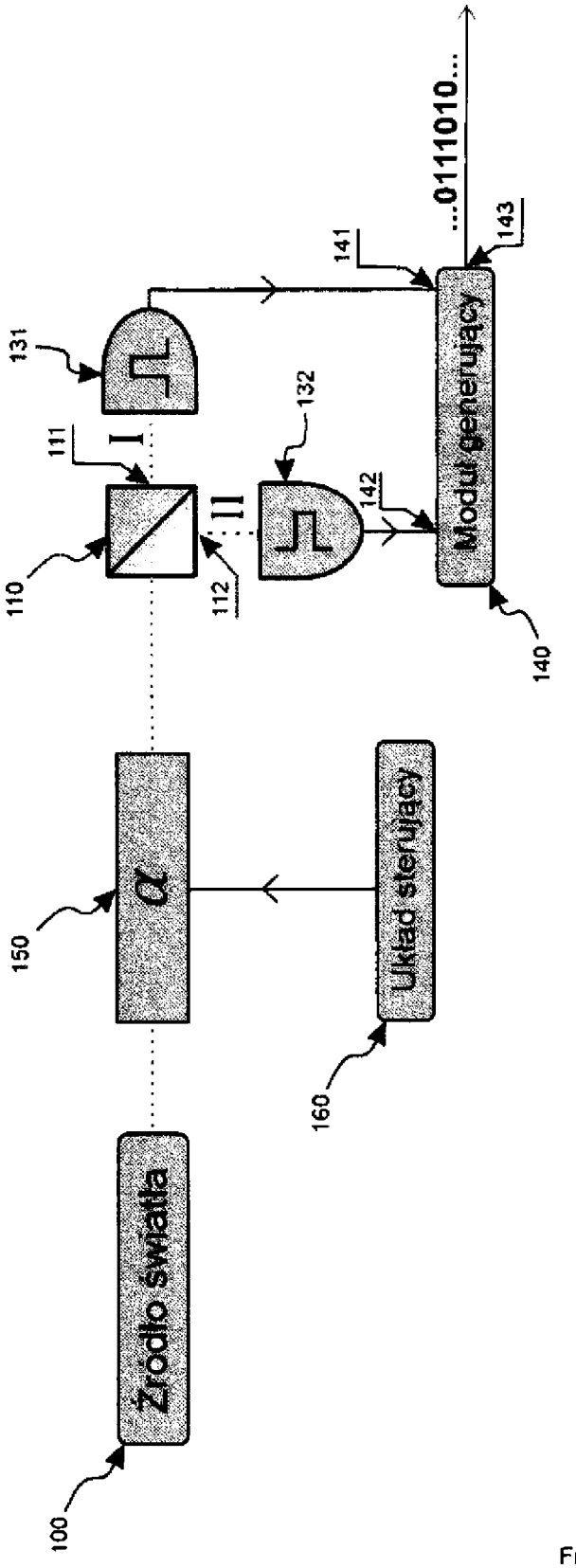
...0111010...
143
141
131
132
111
142
110
112
Moduł generujący
140
150
α
Układ sterujący
160
Źródło światła
100

Fig. 3

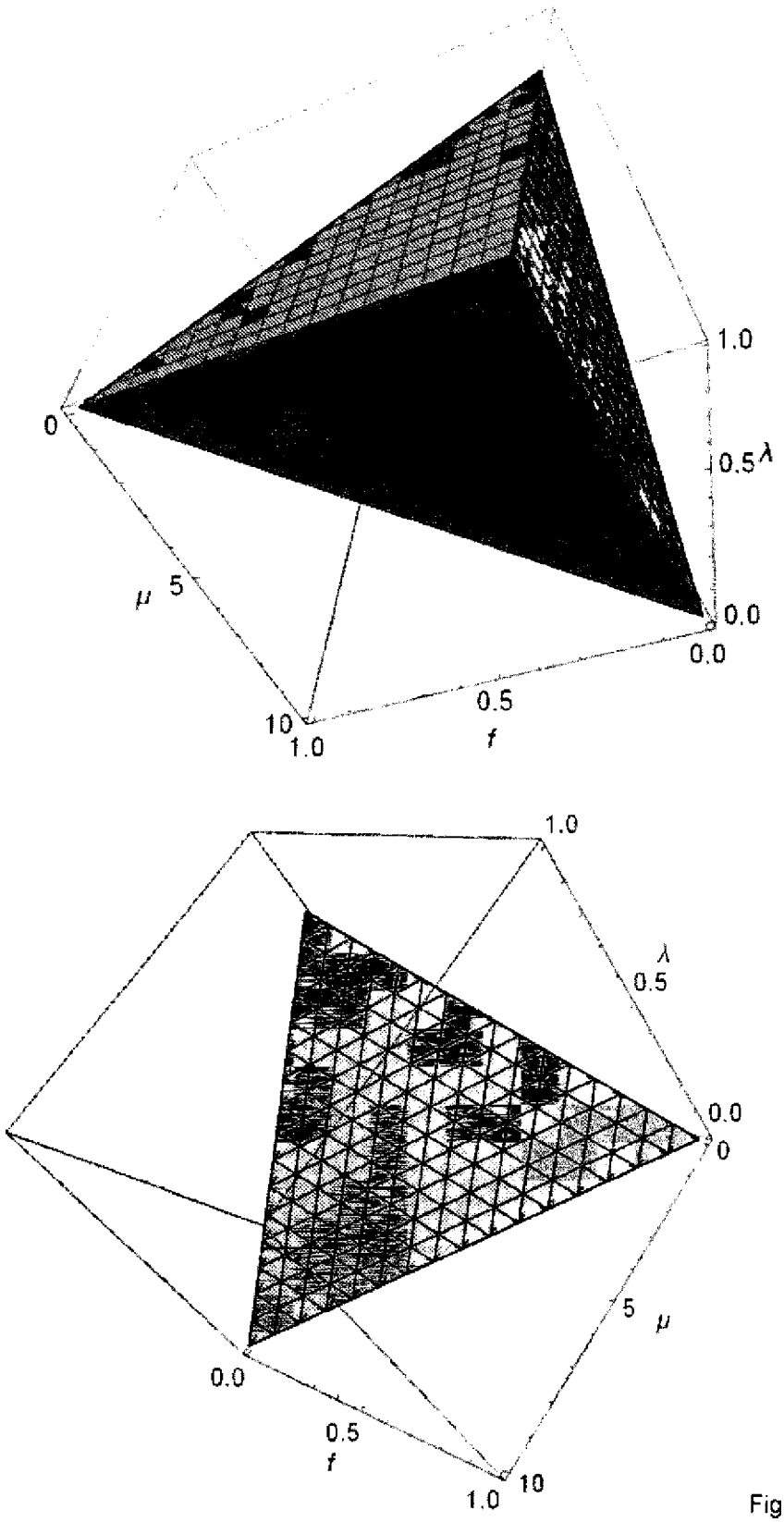

Fig. 4