(19) österreichisches patentamt

(10) **AT 523718 B1 2021-11-15**

(12) **Patentschrift**

(21) Anmeldenummer: A 50521/2020
(22) Anmeldetag: 18.06.2020
(45) Veröffentlicht am: 15.11.2021

(51) Int. Cl.: ***G06F 7/58*** (2006.01)
H01S 5/065 (2006.01)
H03K 3/84 (2006.01)

(56) Entgegenhaltungen:
DE 19826802 C2
US 2015331672 A1
US 2013036145 A1

(73) Patentinhaber:
AIT Austrian Institute of Technology GmbH
1210 Wien (AT)

(74) Vertreter:
Wildhack & Jellinek Patentanwälte OG
1030 Wien (AT)

AT 523718 B1 2021-11-15

(54) **Anordnung zur Erzeugung eines Zufallssignals**

(57) Die Erfindung betrifft eine Anordnung (100) zur Erzeugung eines Zufallssignals umfassend

- eine optische Quelle (4), insbesondere einen Laser,
- einen polarization-multiplexed in-phase/quadrature Modulator (10), der folgende Bestandteile umfasst:
  - o einen optischen Modulatoreingang (101), an den die optische Quelle (4) angeschlossen ist,
  - o zumindest einen nested Mach-Zehnder-Modulator (1), wobei der zumindest eine nested Mach-Zehnder-Modulator (1) dem optischen Modulatoreingang (101) nachgeschaltet ist und
    wobei der zumindest eine nested Mach-Zehnder-Modulator (1) einen optischen Ausgang (15) und zumindest einen elektrischen Eingang (16) zur Vorgabe des Realteils und/oder des Imaginärteils eines optischen Signals aufweist,
- eine Steuereinheit (3), die an den elektrischen Eingang (16) des nested Mach-Zehnder-Modulators (1) angeschlossen ist, wobei die Steuereinheit (3) dazu ausgebildet ist, zumindest einen Arbeitspunkt des polarization-multiplexed inphase/ quadrature Modulators (100) vorzugeben, wobei

zumindest eine Monitorphotodiode (5) dem polarization-multiplexed in-phase/quadrature Modulator (10) nachgeschaltet ist, wobei die Monitorphotodiode (5) dem optischen Ausgang (15) des nested Mach-Zehnder-Modulators (1) nachgeschaltet ist und einen elektrischen Monitorphotodiodenausgang (52) aufweist, sodass ein vom nested Mach-Zehnder-Modulator (1) bereitgestelltes optisches Signal in ein elektrisches Signal umwandelbar ist,
und der Monitorphotodiodenausgang (52) der Monitorphotodiode (5) einen Zufallsausgang (12) der Anordnung (100) zur Bereitstellung eines erzeugten Zufallssignals, insbesondere erzeugter Zufallszahlen, bildet.

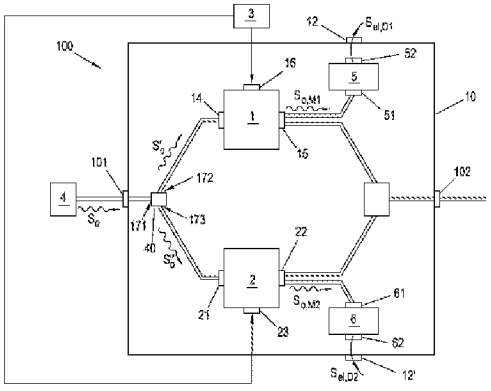


Fig. 1

Beschreibung

[0001] Die Erfindung betrifft eine Anordnung zur Erzeugung eines Zufallssignals gemäß Patentanspruch 1, sowie ein Verfahren zur Erzeugung eines Zufallssignals gemäß Patentanspruch 16.

[0002] Die Sicherheit vieler Anwendungen aus der Informations- und Kommunikationstechnologie wie Datenverschlüsselung oder digitalen Signaturen basiert auf einem Zufallssignal bzw. Zufallszahlen als Grundlage. Daher ist ein Zufallssignal höchster Qualität erforderlich, um digitale Sicherheit zu garantieren. Quanten-Zufallszahlengenerierung kann dabei als wichtiges Werkzeug dienen, um ein derartiges Zufallssignal bereitzustellen, da Quantenzustände inhärent unbestimmt sind und daher eine Entropiequelle darstellen.

[0003] Aufgabe der Erfindung ist es daher, eine Anordnung und ein Verfahren zur Erzeugung eines Zufallssignals bereitzustellen, mit denen ein nicht vorhersagbares Zufallssignal und somit ein Zufallssignal höchster Qualität erzeugt werden kann.

[0004] Die Erfindung löst diese Aufgabe mit einer Anordnung zur Erzeugung eines Zufallssignals gemäß Patentanspruch 1 umfassend
- eine optische Quelle, insbesondere einen Laser,
- einen polarization-multiplexed in-phase/quadrature Modulator, der folgende Bestandteile umfasst:
    - einen optischen Modulatoreingang, an den die optische Quelle angeschlossen ist,
    - zumindest einen nested Mach-Zehnder-Modulator, wobei der zumindest eine nested Mach-Zehnder-Modulator (1) dem optischen Modulatoreingang nachgeschaltet ist und wobei der zumindest eine nested Mach-Zehnder-Modulator einen optischen Ausgang und zumindest einen elektrischen Eingang zur Vorgabe des Realteils und/oder des Imaginärteils eines optischen Signals aufweist, und

- eine Steuereinheit, die an den elektrischen Eingang des nested Mach-Zehnder-Modulators angeschlossen ist, wobei die Steuereinheit dazu ausgebildet ist, zumindest einen Arbeitspunkt des polarization-multiplexed in-phase/quadrature Modulators vorzugeben.

[0005] Erfindungsgemäß ist dabei vorgesehen, dass
- zumindest eine Monitorphotodiode dem polarization-multiplexed in-phase/quadrature Modulator nachgeschaltet ist, wobei die Monitorphotodiode dem optischen Ausgang des nested Mach-Zehnder-Modulators nachgeschaltet ist und einen elektrischen Monitorphotodiodenausgang aufweist, sodass ein vom nested Mach-Zehnder-Modulator bereitgestelltes optisches Signal in ein elektrisches Signal umwandelbar ist, und

dass der Monitorphotodiodenausgang der Monitorphotodiode einen Zufallsausgang der Anordnung zur Bereitstellung eines erzeugten Zufallssignals, insbesondere erzeugter Zufallszahlen, bildet.

[0006] Bei einer derartigen Anordnung werden vorteilhafterweise die Quanteneigenschaften von Licht genutzt, um ein Zufallssignal zu erzeugen. Dabei wird ein bekannter optischer I/Q-Modulator genutzt, der häufig in bekannten kohärenten Übertragungssystemen genutzt wird, um das nicht vorhersagbare Zufallssignal zu erstellen, und mit Monitorphotodioden kombiniert.

[0007] Somit ist kein separates und hochspezifisches Sub-System für die Generierung von Zufallssignalen höchster Qualität erforderlich, da die in kommeriziellen Übertragungssystemen bereits vorhandenen Komponenten zusätzlich für diese Aufgabe verwendet werden können. Es ist lediglich eine geringfügige Änderung in der elektrischen Domäne notwendig, welche im Vergleich zu einer Änderung der Optoelektronik jedoch im Allgemeinen viel einfacher und kosteneffizienter durchzuführen ist.

[0008] Weitere vorteilhafte Ausgestaltungen der Erfindung werden in den Merkmalen der abhängigen Ansprüche beschrieben:

[0009] Gemäß einer vorteilhaften Ausführungsform der Erfindung kann vorgesehen sein,
- dass der polarization-multiplexed in-phase/quadrature Modulator einen Eingangs-Strahlteiler

aufweist, wobei der optische Modulatoreingang an den Eingang des Eingangs-Strahlteilers geführt ist, und wobei ein erster Ausgang des Eingangs-Strahlteilers an den optischen Eingang des nested Mach-Zehnder-Modulators geführt ist und
- dass die Anordnung einen weiteren nested Mach-Zehnder-Modulator umfasst, wobei ein zweiter Ausgang des Eingangs-Strahlteilers an den optischen Eingang des weiteren nested Mach-Zehnder-Modulator geführt ist und wobei der weitere nested Mach-Zehnder-Modulator einen optischen Ausgang und zumindest einen elektrischen Eingang zur Vorgabe des Realteils und/oder des Imaginärteils eines optischen Signals aufweist,
dass die Steuereinheit, gegebenenfalls eine weitere Steuereinheit, an den elektrischen Eingang des weiteren nested Mach-Zehnder-Modulators angeschlossen ist,
dass dem polarization-multiplexed in-phase/quadrature Modulator zumindest eine weitere Monitorphotodiode (6) nachgeschaltet ist, wobei die weitere Monitorphotodiode dem optischen Ausgang des weiteren nested Mach-Zehnder-Modulators nachgeschaltet ist und einen elektrischen Monitorphotodiodenausgang aufweist, sodass ein vom weiteren nested Mach-Zehnder-Modulator bereitgestelltes optisches Signal in ein elektrisches Signal umwandelbar ist, und
dass der Monitorphotodiodenausgang der weiteren Monitorphotodiode (6) einen Zufallsausgang der Anordnung zur Bereitstellung eines erzeugten Zufallssignals, insbesondere erzeugter Zufallszahlen, bildet.

[0010] Gemäß einer vorteilhaften Ausführungsform der Erfindung, durch die ein ungenaues Teilerverhältnis z.B. am Eingangs-Strahlteiler kompensiert werden kann, kann vorgesehen sein, dass die Steuereinheit, und/oder gegebenenfalls die weitere Steuereinheit, dazu ausgebildet ist, die Arbeitspunkte des nested Mach-Zehnder-Modulators und des weiteren nested Mach-Zehnder-Modulators derart vorzugeben, dass der Gleichanteil des Photodiodenstroms der Monitorphotodiode und der weiteren Monitorphotodiode gleich ist.

[0011] Gemäß einer vorteilhaften Ausführungsform der Erfindung kann vorgesehen sein,
- dass die Anordnung einen internen Strahlteiler umfasst, wobei ein erster optischer Ausgang des internen Strahlteilers an den optischen Monitorphotodiodeneingang der Monitorphotodiode angeschlossen ist und/oder
- dass die Anordnung einen weiteren internen Strahlteiler umfasst, wobei ein erster optischer Ausgang des weiteren internen Strahlteilers an den optischen Monitorphotodiodeneingang der weiteren Monitorphotodiode angeschlossen ist.

[0012] Gemäß einer vorteilhaften Ausführungsform der Erfindung kann vorgesehen sein, dass der elektrische Monitorphotodiodenausgang der Monitorphotodiode und der elektrische Monitorphotodiodenausgang der weiteren Monitorphotodiode an eine Umwandlungseinheit angeschlossen sind, wobei der Ausgang der Umwandlungseinheit den Zufallsausgang der Anordnung bildet. Auf diese Weise kann ein elektrisches Zufallssignal bereitgestellt werden.

[0013] Gemäß einer vorteilhaften Ausführungsform der Erfindung zur Bereitstellung eines verstärkten, analogen Zufallssignals, kann vorgesehen sein, dass die Umwandlungseinheit einen Transimpedanzverstärker umfasst,

wobei der Transimpedanzverstärker einen ersten elektrischen Transimpendanzverstärker-Eingang, einen zweiten elektrischen Transimpendanzverstärker-Eingang und einen elektrischen Transimpedanzverstärker-Ausgang aufweist,

wobei der elektrische Monitorphotodiodenausgang der Monitorphotodiode an den ersten elektrischen Transimpendanzverstärker-Eingang angeschlossen ist und wobei der elektrische Monitorphotodiodenausgang der weiteren Monitorphotodiode an den zweiten elektrischen Transimpendanzverstärker-Eingang angeschlossen ist.

[0014] Gemäß einer weiteren vorteilhaften Ausführungsform der Erfindung zur Bereitstellung eines verstärkten, analogen Zufallssignals, kann vorgesehen sein, dass der Transimpedanzverstärker dazu ausgebildet ist, eine Funktion der an den elektrischen Monitorphotodiodenausgängen der Monitorphotodioden anliegenden elektrischen Signale, insbesondere der durch die elektrischen Monitorphotodiodenausgängen der Monitorphotodioden fließenden Ströme, zu bilden und zu verstärken, und derart ein verstärktes, analoges Zufallssignal am Transimpedanzver-

stärker-Ausgang bereitzustellen,
wobei insbesondere vorgesehen ist, dass der Transimpedanzverstärker-Ausgang den Ausgang der Umwandlungseinheit bildet.

[0015] Gemäß einer weiteren vorteilhaften Ausführungsform der Erfindung zur Bereitstellung eines verstärkten, analogen Zufallssignals, kann vorgesehen sein, dass der Transimpedanzverstärker dazu ausgebildet ist, die Differenz der an den elektrischen Monitorphotodiodenausgängen der Monitorphotodioden anliegenden elektrischen Signale, insbesondere der durch die elektrischen Monitorphotodiodenausgängen der Monitorphotodioden fließenden Ströme, zu bilden.

[0016] Gemäß einer vorteilhaften Ausführungsform der Erfindung zur Bereitstellung eines verstärkten, analogen Zufallssignals mit verbesserter Signalqualität kann vorgesehen sein, die Umwandlungseinheit eine analoge Signalverarbeitungseinheit umfasst, wobei die analoge Signalverarbeitungseinheit einen elektrischen Eingang und einen elektrischen Ausgang aufweist und
wobei der elektrische Transimpedanzverstärker-Ausgang an den elektrischen Eingang der analogen Signalverarbeitungseinheit angeschlossenen ist,
wobei die analoge Signalverarbeitungseinheit dazu ausgebildet ist, das am Transimpedanzverstärker-Ausgang bereitgestellte verstärkte, analoge Zufallssignal zu filtern und am elektrischen Ausgang der analogen Signalverarbeitungseinheit bereitzustellen,
wobei insbesondere vorgesehen ist, dass der elektrische Ausgang der analogen Signalverarbeitungseinheit den Ausgang der Umwandlungseinheit bildet.

[0017] Gemäß einer vorteilhaften Ausführungsform der Erfindung zur Bereitstellung eines binären Zufallssignals kann vorgesehen sein, dass die Umwandlungseinheit einen Analog-Digital-Wandler umfasst, wobei der Analog-Digital-Wandler einen elektrischen Wandlereingang einen elektrischen Wandlerausgang aufweist und
wobei der elektrische Transimpedanzverstärker-Ausgang an den elektrischen Wandlereingang des Analog-Digital-Wandlers, insbesondere an den der elektrische Ausgang der analogen Signalverarbeitungseinheit, angeschlossenen ist,
wobei der Analog-Digital-Wandler dazu ausgebildet ist, auf Grundlage des am Transimpedanzverstärker-Ausgang, insbesondere am elektrischen Ausgang der analogen Signalverarbeitungseinheit, bereitgestellten verstärkten, analogen Zufallssignal ein binäres Zufallssignal zu erzeugen und am elektrischen Wandlerausgang bereitzustellen, wobei insbesondere vorgesehen ist, dass der elektrische Wandlerausgang den Ausgang der Umwandlungseinheit bildet.

[0018] Gemäß einer vorteilhaften Ausführungsform der Erfindung zur Bereitstellung eines binären Zufallssignals mit verbesserten statistischen Eigenschaften kann vorgesehen sein, dass die Umwandlungseinheit eine digitale Signalverarbeitungseinheit umfasst, wobei die digitale Signalverarbeitungseinheit einen elektrischen Signaleingang und einen elektrischen Signalausgang aufweist und
wobei der elektrische Wandlerausgang an den elektrischen Signaleingang der digitalen Signalverarbeitungseinheit angeschlossen ist, und
wobei die digitale Signalverarbeitungseinheit dazu ausgebildet ist, aus dem am elektrische Wandlerausgang bereitgestellten binären Zufallssignal ein binäres Zufallssignal, insbesondere eine Zufallszahl, mit im Vergleich zur Entropie des vom Analog-Digital-Wandler bereitgestellten binären Zufallssignals verbesserten statistischen Eigenschaften zu erzeugen und an ihrem elektrischen Signalausgang bereitzustellen,
wobei insbesondere vorgesehen ist, dass der elektrische Signalausgang der digitalen Signalverarbeitungseinheit den Ausgang der Umwandlungseinheit bildet.

[0019] Verbesserte statistische Eigenschaften sind im Zusammenhang mit der Erfindung so zu verstehen, dass entweder

1) eine Entropie des binären Zufallssignals pro Bit Zufallszahl (= eine Entropie des binären Zufallssignals dividiert durch die Länge des binären Zufallssignals in Bit) vergrößert bzw. erhöht wird, oder
2) der statistische Abstand der Wahrscheinlichkeitsverteilung des binären Zufallssignals zu einer vorgegebenen Wahrscheinlichkeitsverteilung reduziert wird, im Vergleich zum binä-

ren Signal bzw. Zufallssignal, das der digitalen Signalverarbeitungseinheit zugeführt wird.

[0020] Dabei ist der statistische Abstand d zweier diskreter Wahrscheinlichkeitsverteilungen X und Y, die über dem gleichen endlichen Alphabet A definiert sind, folgendermaßen definiert:

$$d(X,Y) = \max_{a \in A} |P_X(a) - P_Y(a)|$$

[0021] Der statistische Abstand beschreibt den maximalen Unterschied der Wahrscheinlichkeit P ein bestimmtes Ergebnis zu erhalten. Dabei sind zwei Verteilungen X und Y ε-close (ε-nahe), wenn

$$d(X,Y) < \epsilon$$

gilt.

[0022] Gemäß einer weiteren vorteilhaften Ausführungsform der Erfindung zur Bereitstellung eines binären Zufallssignals mit verbesserten statistischen Eigenschaften kann vorgesehen sein, dass die Umwandlungseinheit einen Entropieschätzer umfasst, wobei der Entropieschätzer dazu ausgebildet ist, aus dem bekannten Verhalten der optischen Komponenten der Anordnung, insbesondere der optischen Quelle und/oder des polarization-multiplexed in-phase/quadrature Modulators, und der elektrischen Komponenten der Anordnung, insbesondere der Steuereinheit und/oder des Transimpedanzverstärkers und/oder des Analog-Digital-Wandlers, eine Entropie, insbesondere die Shannon-Entropie oder die Min-Entropie, oder eine bedingte Entropie, insbesondere die bedingte Shannon-Entropie oder die bedingte Min-Entropie, des am elektrischen Wandlerausgang bereitgestellten binären Zufallssignals zu berechnen und zur Verfügung zu halten.

[0023] Gemäß einer weiteren vorteilhaften Ausführungsform der Erfindung zur Bereitstellung eines binären Zufallssignals mit verbesserten statistischen Eigenschaften kann vorgesehen sein, dass die Umwandlungseinheit einen Entropieschätzer umfasst, wobei der Entropieschätzer dazu ausgebildet ist, aus dem bekannten Verhalten der optischen Komponenten der Anordnung, insbesondere der optischen Quelle und/oder des polarization-multiplexed in-phase/quadrature Modulators, und der elektrischen Komponenten der Anordnung, insbesondere der Steuereinheit und/oder des Transimpedanzverstärkers und/oder des Analog-Digital-Wandlers, sowie anhand vorgegebener Parameter, insbesondere anhand einer vorgegebenen unteren Schranke für eine Entropie, eine parametrisierte Entropie, insbesondere die epsilon-smooth Min-Entropie, oder eine parametrisierte bedingte Entropie, insbesondere die bedingte epsilon-smooth Min-Entropie, des am elektrischen Wandlerausgang bereitgestellten binären Zufallssignals zu berechnen und zur Verfügung zu halten.

[0024] Gemäß einer weiteren vorteilhaften Ausführungsform der Erfindung zur Bereitstellung eines binären Zufallssignals mit verbesserten statistischen Eigenschaften kann vorgesehen sein, dass die digitale Signalverarbeitungseinheit dazu ausgebildet ist, die vom Entropieschätzer bestimmte Entropie heranzuziehen, um eine Zufallszahl mit definierter Entropie pro bit, insbesondere mit einer Entropie möglichst nahe an 1 bit pro bit, nach einem Zufallszahlenextraktionsverfahren, insbesondere mittels von Neumann-Extraktion, zu erzeugen und an ihrem elektrischen Signalausgang bereitzustellen.

[0025] Unter einer Zufallsvariable mit definierter Entropie pro bit wird im Zusammenhang mit der Erfindung auch eine Zufallsvariable mit definiertem Minimumwert für eine Entropie pro bit bzw. Block oder mit definiertem Minimumwert für den statistischen Abstand zur Gleichverteilung oder mit definiertem Minimumwert für den statistischen Abstand zu einer anderen gewünschten Wahrscheinlichkeitsverteilung verstanden.

[0026] Gemäß einer weiteren vorteilhaften Ausführungsform der Erfindung zur Bereitstellung eines binären Zufallssignals mit verbesserten statistischen Eigenschaften kann vorgesehen sein, dass die digitale Signalverarbeitungseinheit dazu ausgebildet ist, die vom Entropieschätzer bestimmte Entropie sowie eine vorgegebene, insbesondere in der digitalen Signalverarbeitungseinheit hinterlegte, Zufallszahl heranzuziehen, um eine Zufallszahl mit definierter Entropie pro bit, insbesondere mit einer Entropie möglichst nahe an 1 bit pro bit oder mit einer Verteilung die

epsilon- bzw. ε-nahe an einer Gleichverteilung ist, nach einem Zufallszahlenextraktionsverfahren, insbesondere mittels Universal Hashing und/oder Toeplitz Hashing, zu erzeugen und an ihrem elektrischen Signalausgang bereitzustellen.

[0027] Aufgabe der Erfindung ist es weiters, ein Verfahren zur Erzeugung eines Zufallssignals mit einer Anordnung umfassend eine optische Quelle und einen polarization-multiplexed in-phase/quadrature Modulator, insbesondere einer erfindungsgemäßen Anordnung, bereitzustellen,
- wobei ein optisches Signal aus der optischen Quelle, insbesondere einem Laser, dem optischen Eingang des polarization-multiplexed in-phase/quadrature Modulators zugeführt wird,
- wobei zumindest ein Anteil des am optischen Eingang des polarization-multiplexed in-phase/quadrature Modulator einlangenden optischen Signal an einen nested Mach-Zehnder-Modulator des polarization-multiplexed in-phase/quadrature Modulator weitergeleitet wird,

[0028] Diese Aufgabe wird durch die kennzeichnenden Merkmale des Anspruchs 16 gelöst. Erfindungsgemäß ist dabei vorgesehen,
- dass zumindest ein Anteil des vom nested Mach-Zehnder-Modulator bereitgestellten optischen Ausgangssignals an eine Monitorphotodiode weitergeleitet wird, und
- dass ein Zufallssignal in Form des am elektrischen Monitorphotodiodenausgang der Monitorphotodiode elektrischen Signals bereitgestellt wird.

[0029] Gemäß einer vorteilhaften Ausführungsform der Erfindung zur Bereitstellung eines verbesserten elektrischen Zufallssignals kann vorgesehen sein,
- dass ein weiterer Anteil des am optischen Eingang des polarization-multiplexed in-phase/quadrature Modulator einlangenden optischen Signal an einen weiteren nested Mach-Zehnder-Modulator des polarization-multiplexed in-phase/quadrature Modulators weitergeleitet wird,
- dass zumindest ein Anteil des vom weiteren nested Mach-Zehnder-Modulator bereitgestellten optischen Ausgangssignals an eine weitere Monitorphotodiode weitergeleitet wird, und
- dass ein Zufallssignal in Form des am elektrischen Monitorphotodiodenausgang der weiteren Monitorphotodiode (6) anliegenden elektrischen Signals bereitgestellt wird.

[0030] Gemäß einer vorteilhaften Ausführungsform der Erfindung, durch die ein ungenaues Teilerverhältnis kompensiert werden kann, kann vorgesehen sein, dass die Arbeitspunkte der nested Mach-Zehnder-Modulatoren derart vorgegeben werden, dass der Gleichanteil der Photodiodenströme der beiden Monitorphotodioden gleich ist.

[0031] Gemäß einer vorteilhaften Ausführungsform der Erfindung zur Bereitstellung eines verstärkten analogen Zufallssignals kann vorgesehen sein, dass die an den elektrischen Monitorphotodiodenausgängen der Monitorphotodiode anliegenden elektrischen Signale verknüpft werden, sodass derart ein verstärktes, analoges Zufallssignal bereitgestellt wird, wobei insbesondere vorgesehen ist, dass die Differenz der elektrischen Signale gebildet wird.

[0032] Gemäß einer vorteilhaften Ausführungsform der Erfindung zur Bereitstellung eines binären Zufallssignals kann vorgesehen sein, dass das verstärkte, analoge Zufallssignal, gegebenenfalls gefiltert und, in ein binäres Zufallssignal umgewandelt wird.

[0033] Gemäß einer vorteilhaften Ausführungsform der Erfindung zur Bereitstellung eines verbesserten binären Zufallssignals kann vorgesehen sein, dass die Entropie des binären Zufallssignals ermittelt wird und dass daraus ein binäres Zufallssignal mit verbesserten statistischen Eigenschaften, insbesondere erhöhter Entropie pro bit, vorzugsweise eine Zufallszahl mit erhöhter Entropie, gegebenenfalls unter Einbeziehung einer vorgegebenen Entropiezahl, berechnet wird.

[0034] Gemäß einer vorteilhaften Ausführungsform der Erfindung zur Bereitstellung eines weiter verbesserten binären Zufallssignals kann vorgesehen sein, dass das binäre Zufallssignal mit verbesserten statistischen Eigenschaften, insbesondere erhöhter Entropie pro bit, gegebenenfalls unter Einbeziehung einer vorgegebenen Zufallszahl, nach einem Zufallszahlenextraktionsverfahren, insbesondere mittels von Neumann-Extraktion oder Universal Hashing oder Toeplitz Hashing, berechnet wird.

[0035] Gemäß einer vorteilhaften Ausführungsform der Erfindung zur abwechselnden Bereitstellung eines Zufallssignals und Übermittlung von Daten kann vorgesehen sein, dass der polarization-multiplexed in-phase/quadrature Modulator zwei Betriebszustände aufweist,

- wobei im ersten Betriebszustand ein Datensignal über den optischen Ausgang des polarization-multiplexed in-phase/quadrature Modulators übertragen wird und
- wobei im zweiten Betriebszustand zumindest ein Zufallssignal, insbesondere Zufallszahlen, nach einem erfindungsgemäßen Verfahren erzeugt werden und

dass zwischen zwei Betriebszuständen gewechselt wird indem der Arbeitspunkt des polarization-multiplexed in-phase/quadrature Modulators geändert wird.

[0036] Gemäß einer vorteilhaften Ausführungsform der Erfindung zur gleichzeitigen Bereitstellung eines Zufallssignals und Übermittlung von Daten kann vorgesehen sein, dass die beiden Betriebszustände gleichzeitig genutzt werden, wobei der Frequenzbereich des polarization-multiplexed in-phase/quadrature Modulators derart aufgeteilt wird, sodass der Frequenzbereich des Datensignals und der Frequenzbereich des zumindest einen Zufallssignals, insbesondere der Zufallszahlen, einander nicht überlappen, sodass ein Übersprechen zwischen den beiden Signalen unterdrückt wird.

[0037] Weitere Vorteile und Ausführungsformen der Erfindung ergeben sich aus der Beschreibung und den beiliegenden Zeichnungen.

[0038] Besonders vorteilhafte, aber nicht einschränkend zu verstehende Ausführungsbeispiele der Erfindung werden im Folgenden anhand der beiliegenden Zeichnungen schematisch dargestellt und unter Bezugnahme auf die Zeichnungen beispielhaft beschrieben.

[0039] Im Folgenden zeigen schematisch:

[0040] Fig. 1 ein erstes Ausführungsbeispiel einer erfindungsgemäßen Anordnung,

[0041] Fig. 2 ein Ausführungsbeispiel eines nested Mach-Zehnder-Modulators,

[0042] Fig. 3 ein zweites Ausführungsbeispiel einer erfindungsgemäßen Anordnung,

[0043] Fig. 4 eine Detailansicht der Umwandlungseinheit der Anordnung aus Fig. 3.

[0044] Fig. 1 und Fig. 3 zeigen zwei Ausführungsbeispiele einer erfindungsgemäßen Anordnung 100. Ein drittes, besonders einfach aufgebautes, Ausführungsbeispiel einer erfindungsgemäßen Anordnung 100 wird weiter unten ohne eigene Figur beschrieben. In allen Ausführungsbeispielen einer erfindungsgemäßen Anordnung 100 wird ein polarization-multiplexed in-phase/quadrature Modulator 10 zur Erzeugung eines Zufallssignals eingesetzt. Die Bezeichnung „polarization-multiplexed" bezieht sich dabei auf die Betriebsart des in-phase/quadrature Modulators. Dies bedeutet, dass die durch den in-phase/quadrature Modulator 10 für die Übertragung von Daten vorgesehene Quadraturamplitudenmodulation in beiden Polarisationsebenen des Lichts durchgeführt wird, d.h. im Polarisationsmultiplex. Da beim Empfänger kohärente Detektion der übermittelten Daten durchgeführt wird, um diese vom optischen in den elektrischen Bereich rückzuführen, ist aufgrund der Polarisationsempfindlichkeit der Detektionsmethode ein geeignetes Management der Lichtpolarisation erforderlich. Diese wird typischerweise durch kohärente Detektion in beiden Polarisationsebenen bewerkstelligt. Somit ergibt sich auch kein Nachteil im Sinn von Komplexität, am Sender beide Polarisationsebenen zu verwenden, während neben der somit erzielten polarisationsunabhängigen Detektion auch die Datenrate verdoppelt werden kann. Die Komponenten eines derartigen polarization-multiplexed in-phase/quadrature Modulators 10 werden im Folgenden näher erläutert.

[0045] Der polarization-multiplexed in-phase/quadrature Modulator 10 in Fig. 1 und Fig. 3 bzw. im dritten Ausführungsbeispiel weist einen optischen Modulatoreingang 101 auf, an den eine optische Quelle 4 angeschlossen ist, bei der es sich, wie im Ausführungsbeispiel in Fig. 1 um einen Laser handeln kann.

[0046] Ein weiterer Bestandteil des polarization-multiplexed in-phase/quadrature Modulators 10 ist zumindest ein nested Mach-Zehnder-Modulator 1. Ein derartiger nested Mach-Zehnder-Modulator 1 ist beispielsweise in der US 2011/170161 A1 beschrieben und umfasst einen optischen

Eingang 14, einen optischen Ausgang 15 und zumindest einen elektrischen Eingang 16.

AUSFÜHRUNGSBEISPIEL EINES NESTED MACH-ZEHNDER-MODULATORS 1, FIG. 2

[0047] Jeder derartige nested Mach-Zehnder-Modulator 1 umfasst ein Mach-Zehnder-Interferometer-Paar $MZI_{1,a}$, $MZI_{1,b}$, an seinem optischen Eingang 14 einen optischen Strahlteiler ST, z.B. einen optical intensity splitter, und an seinem optischen Ausgang 15 einen optischen Kombinierer SC, z.B. einen optical intensity combiner.

[0048] Vom optischen Eingang 14 gelangen optische Signale über den optischen Strahlteiler ST zum jeweiligen Mach-Zehnder-Interferometer $MZI_{1,a}$, $MZI_{1,b}$. Jedem Mach-Zehnder-Interferometer $MZI_{1,a}$, $MZI_{1,b}$ wird somit ein optisches Signal zugeführt, das auf ein entsprechendes, den optischen Strahlteiler ST am optischen Eingang 14 des nested Mach-Zehnder-Modulators 1, verlassendes, optisches Signal zurückgeht. Jedes Mach-Zehnder-Interferometer $MZI_{1,a}$, $MZI_{1,b}$ erzeugt weiters ein optisches Signal, das durch Kombination der, von den beiden Mach-Zehnder-Interferometern $MZI_{1,a}$, $MZI_{1,b}$ bereitgestellten optischen Signale, im optischen Kombinierer SC am optischen Ausgang 15 des nested Mach-Zehnder-Modulators 1 entsteht.

[0049] Der optische Strahlteiler ST am optischen Eingang 14 des nested Mach-Zehnder-Modulators 1 und der optische Kombinierer SC am optischen Ausgang 15 des nested Mach-Zehnder-Modulators 1 können z.B. konventionelle 50/50-Strahlteiler (optical intensity coupler) oder asymmetrische und/oder verstimmbare optische Kombinierer sein.

[0050] Jeder nested Mach-Zehnder-Modulator 1 weist insgesamt drei Masseelektroden GE_1, ..., GE_3 und zwei Steuerelektroden DE_1, DE_2 auf.

[0051] Jedes Mach-Zehnder-Interferometer $MZI_{1,a}$, $MZI_{1,b}$ eines nested Mach-Zehnder-Modulators 1 weist jeweils ein Paar interner optischer Arme IA_1, IA_2; IA_3, IA_4 auf, denen jeweils eine Masseelektrode GE_1; DE_3 zugeordnet ist. Jede Steuerelektrode DE_1, DE_2 ist jeweils einem Mach-Zehnder-Interferometer $MZI_{1,a}$, $MZI_{1,b}$ zugeordnet und zwischen dessen optischen Armen IA_1, IA_2; IA_3, IA_4 angeordnet. Zwei der drei Masseelektroden, in Fig. 2 sind dies die Masseelektroden GE_1 und GE_3, sind jeweils nur einem Mach-Zehnder-Interferometer zugeordnet, während eine der Masseelektroden, in Fig. 2 ist dies die Masseelektrode GE_2, von beiden Mach-Zehnder-Interferometern $MZI_{1,a}$, $MZI_{1,b}$ des nested Mach-Zehnder-Modulators 1 geteilt wird.

[0052] Weiters weist jedes Mach-Zehnder-Interferometer $MZI_{1,a}$, $MZI_{1,b}$ des nested Mach-Zehnder-Modulators 1 jeweils einen eigenen optischen Strahlteiler $OS_{1,a}$, $OS_{1,b}$, bzw. optischen Splitter, und jeweils einen eigenen optischen Kombinierer $OC_{1,a}$, $OC_{1,b}$ auf, die jeweils mit den optischen Armen IA_1, IA_2; IA_3, IA_4 des jeweiligen Mach-Zehnder Interferometers $MZI_{1,a}$, $MZI_{1,b}$ verbunden sind. Jeder optische Arm IA_1, IA_2; IA_3, IA_4 jedes der Mach-Zehnder-Interferometer $MZI_{1,a}$, $MZI_{1,b}$ des nested Mach-Zehnder-Modulators 1 besitzt einen optischen phase shifter, der pro optischem Arm IA_1, IA_2; IA_3, IA_4 Halbleiterverzweigungen $V_{1,a}$, $V_{1,b}$; $V_{2,a}$, $V_{2,b}$ und ein Elektrodenpaar GE_1, DE_1; DE_1, GE_2; GE_2, DE_2; DE_2, GE_3 aufweist.

[0053] Bei diesem Elektrodenpaar GE_1, DE_1; DE_1, GE_2; GE_2, DE_2; DE_2, GE_3 handelt es sich um eine Kombination aus Steuerelektrode DE_1, DE_2 und Masseelektrode GE_1, ..., GE_3, wie oben beschrieben. Über diese Elektroden werden elektrische Spannungen an den Halbleiterverzweigungen $V_{1,a}$, $V_{1,b}$; $V_{2,a}$, $V_{2,b}$ angelegt, um die optischen phase shifters der internen optischen Arme IA_1, IA_2; IA_3, IA_4 jedes Mach-Zehnder-Interferometers $MZI_{1,a}$, $MZI_{1,b}$ zu steuern. Die zentral angeordnete Steuerelektrode DE_1, DE_2 steuert dabei den optischen phase shifter des jeweiligen Mach-Zehnder-Interferometers $MZI_{1,a}$, $MZI_{1,b}$.

[0054] Ein optisches Trägersignal kann an einem der optischen Eingänge eines der Mach-Zehnder-Interferometer $MZI_{1,a}$, $MZI_{1,b}$ des nested Mach-Zehnder-Modulators 1 empfangen werden. Dieses optische Trägersignal kann ein unmodulierter, kontinuierlicher, kohärenter Lichtstrahl sein, der von einem Laser ausgesendet werden kann. Alternativ dazu kann es sich, wie in Fig. 1, um einen kohärenten Lichtstrahl handeln, der von einer anderen optischen Komponente wie einem Strahlteiler bzw. einem optical intensity splitter oder auch von einem anderen optischen Modulator stammen kann.

[0055] Die Halbleiterverzweigungen $V_{1,a}$, $V_{1,b}$; $V_{2,a}$, $V_{2,b}$ in den beiden Armen IA_1, IA_2; IA_3, IA_4 des jeweiligen Mach-Zehnder-Interferometers $MZI_{1,a}$, $MZI_{1,b}$ werden elektrisch angesteuert, einen einlangenden Strom an Datensymbolen auf das optische Trägersignal aufzumodulieren. Dabei kann ein Gegenstück eines Datensignals an einer zentralen Steuerelektrode DE_1, DE_2 zugeführt werden, während das Datensignal an der jeweils anderen zentralen Steuerelektrode DE_1, DE_2 zugeführt wird. Es kann auch an einer zentralen Steuerelektrode DE_1, DE_2 eine Spannung angelegt werden, während an der jeweils anderen zentralen Steuerelektrode DE_1, DE_2 eine Spannung mit gegenteiligem Vorzeichen angelegt wird.

[0056] Am elektrischen Eingang 16 des nested Mach-Zehnder-Modulators 1 können also elektrische Signale vorgegeben werden, mit denen der Arbeitspunkt des nested Mach-Zehnder-Modulators 1 eingestellt und der Realteils und/oder der Imaginärteil des optischen Signals beeinflusst werden können.

ERSTES AUSFÜHRUNGSBEISPIEL EINER ERFINDUNGSGEMÄßEN ANORDNUNG 100, FIG. 1

[0057] Der polarization-multiplexed in-phase/quadrature Modulator 10 im ersten Ausführungsbeispiel in Fig. 1 umfasst einen Eingangs-Strahlteiler 40, der einen Eingang 171, einen ersten Ausgang 172 und einen zweiten Ausgang 173 besitzt. Der optische Modulatoreingang 101 ist an den Eingang 171 des Eingangs-Strahlteilers 40 geführt.

[0058] Der erste Ausgang 172 des Eingangs-Strahlteilers 40 des polarization-multiplexed in-phase/quadrature Modulator 10 ist im ersten Ausführungsbeispiel gezeigt in Fig. 1 an den optischen Eingang 14 des nested Mach-Zehnder-Modulators 1 geführt.

[0059] Über den elektrischen Eingang 16 des nested Mach-Zehnder-Modulators 1 werden im ersten Ausführungsbeispiel einer erfindungsgemäßen Anordnung 100 von einer Steuereinheit 3 die elektrische Signale vorgegeben, mit denen der Arbeitspunkt des nested Mach-Zehnder-Modulators 1 eingestellt wird.

[0060] Eine Monitorphotodiode 5 ist dem optischen Ausgang 15 des nested Mach-Zehnder-Modulators 1, nachgeschaltet. Im ersten Ausführungsbeispiel wird die Monitorphotodiode 5 durch einen zum optischen Datenausgang des nested Mach-Zehnder-Modulators 1 komplementären Mach-Zehnder-Interferometer-Ausgang des nested Mach-Zehnder-Modulators 1 angespeist. Dies ist schematisch durch die beiden, aus dem optischen Ausgang 15 des nested Mach-Zehnder-Modulators 1 führenden optischen Pfade in Fig. 1 angedeutet.

[0061] Die Monitorphotodiode 5 kann jedoch auch auf andere Weise dem polarization-multiplexed in-phase/quadrature Modulator 10 bzw. dem optischen Ausgang 15 des nested Mach-Zehnder-Modulators 1, nachgeschaltet sein. Dies kann z.B. über Einfügen eines Strahlteilers erfolgen, d.h. es werden typischerweise z.B. 10% des optischen Ausgangs 15 auf die Monitorphotodiode 5 abgezweigt. Dies wird im Zusammenhang mit dem optisches Signal S_o der optischen Quelle 4 auf Seite 16 bzw. Fig. 3 noch näher erläutert. Auf weitere Möglichkeiten wird im Zusammenhang mit dem zweiten und dritten Ausführungsbeispiel weiter unten näher eingegangen.

[0062] Wie zuvor bereits beschrieben, stellt jedes Mach-Zehnder-Interferometer $MZI_{1,a}$, $MZI_{1,b}$ zwei Ausgänge bereit, die komplementär wirken, d.h. ein Ausgang erfährt konstruktive, der andere destruktive Interferenz. Dabei kann es sich z.B. um den Ausgang OC1,a und einen weiteren, in Fig. 2 nicht eingezeichneten Ausgang OC1,a* handeln, der nicht nach rechts unten in Richtung des optischen Kombinierers SC abzweigt, sondern nach rechts oben in Richtung einer Monitorphotodiode. Im Fall, dass die Monitorphotodiode 5 am komplementären Ausgang angeschlossen ist, steht der jeweils andere, optische Ausgang des jeweiligen Mach-Zehnder-Interferometers $MZI_{1,a}$, $MZI_{1,b}$ des nested Mach-Zehnder-Modulators 1 z.B. für Datenübertragung komplementär zum Montiorphotodiodeneingang 51 der Monitorphotodiode 5 zur Verfügung. In diesem Fall wird der Arbeitspunkt des nested Mach-Zehnder-Modulators 1 so eingestellt, dass am optischen Ausgang des jeweiligen Mach-Zehnder-Interferometers $MZI_{1,a}$, $MZI_{1,b}$ minimale Leistung abgegeben wird, sodass am Monitorphotodiodeneingang 51 der Monitorphotodiode 5 maximale Leistung auf-

tritt, da die beiden Ausgänge der Mach-Zehnder-Interferometer $MZI_{1,a}$, $MZI_{1,b}$ komplementär, also gegenläufig ausgebildet sind.

[0063] Die Monitorphotodiode 5 weist einen elektrischen Monitorphotodiodenausgang 52 auf, der in der einfachen Ausgestaltung einer erfindungsgemäßen Anordnung 100, wie sie in Fig. 1 dargestellt ist, einen Zufallsausgang 12 der Anordnung 100 bildet. An diesem Zufallsausgang 12 kann ein erzeugtes, analoges Zufallssignal, insbesondere erzeugte Zufallszahlen, bereitgestellt werden.

[0064] Die Kombination einer derartigen Monitorphotodiode 5 mit einem polarization-multiplexed in-phase/quadrature Modulator 10 und einer optischen Quelle 4 ermöglicht es vorteilhafterweise, den zufälligen Charakter des von der optischen Quelle 4 ausgesandten Lichts für die Erzeugung eines Zufallssignals zu verwenden. Auf konkrete Ausführungsbeispiele eines erfindungsgemäßen Verfahrens wird weiter unten näher eingegangen.

[0065] Optional ist es auch möglich, dass die Anordnung 100, wie in Fig. 1, einen weiteren nested Mach-Zehnder-Modulator 2 aufweist, der denselben Aufbau wie der nested Mach-Zehnder-Modulator 1, der oben beschrieben wurde, aufweist. Der zweite Ausgang 173 des Eingangs-Strahlteilers 40 kann in diesem Fall, wie im ersten Ausführungsbeispiel in Fig. 1, an den optischen Eingang 21 des weiteren nested Mach-Zehnder-Modulators 2 geführt sein.

[0066] Wenn die erfindungsgemäße Anordnung 100 wie in Fig. 1 und Fig. 3 zwei nested Mach-Zehnder-Modulatoren 1, 2 umfasst, ist das Vorhandensein eines Eingangs-Strahlteilers 40 besonders vorteilhaft, da in diesem Fall beide nested Mach-Zehnder-Modulatoren 1, 2 gleichzeitig für die Erzeugung von Zufallssignalen herangezogen werden können.

[0067] Der weitere nested Mach-Zehnder-Modulator 2 weist wie der nested Mach-Zehnder-Modulator 1 einen optischen Ausgang 22 und zumindest einen elektrischen Eingang 23 auf, der zur Einstellung des Arbeitspunktes des weiteren nested Mach-Zehnder-Modulators 2 und somit zur Vorgabe des Realteils und/oder des Imaginärteil des optischen Ausgangssignals dient, das den weiteren nested Mach-Zehnder-Modulator 2 verlässt.

[0068] Über den elektrischen Eingang 23 des weiteren nested Mach-Zehnder-Modulators 2 werden im ersten Ausführungsbeispiel einer erfindungsgemäßen Anordnung 100 von der Steuereinheit 3 die elektrische Signale vorgegeben, mit denen auch der Arbeitspunkt des nested Mach-Zehnder-Modulators 1 eingestellt wird. Optional ist es auch möglich, dass eine von der Steuereinheit 3 verschiedene, weitere Steuereinheit den weiteren nested Mach-Zehnder-Modulator 2 über den elektrischen Eingang 23 ansteuert.

[0069] Im ersten Ausführungsbeispiel ist eine weitere Monitorphotodiode 6 dem polarization-multiplexed in-phase/quadrature Modulator 10 nachgeschaltet, bzw. an den optischen Ausgang 22 des weiteren nested Mach-Zehnder-Modulators 2 angeschlossen. Wie die Monitorphotodiode 5 ist auch die weitere Monitorphotodiode 6 durch einen zum optischen Datenausgang des weiteren nested Mach-Zehnder-Modulators 2 komplementären Mach-Zehnder-Interferometer-Ausgang des weiteren nested Mach-Zehnder-Modulators 2 angespeist. Dies ist schematisch durch die beiden, aus dem optischen Ausgang 22 des weiteren nested Mach-Zehnder-Modulators 2 führenden optischen Pfade in Fig. 1 angedeutet. Der Arbeitspunkt des weiteren nested Mach-Zehnder-Modulators 2 wird dabei auf dieselbe Weise eingestellt, wie dies für die Monitorphotodiode 5 weiter oben beschrieben wurde.

[0070] Die weitere Monitorphotodiode 6 weist einen elektrischen Monitorphotodiodenausgang 62 auf. Der elektrische Monitorphotodiodenausgang 62 kann in einer einfachen Ausgestaltung einer erfindungsgemäßen Anordnung 100 einen weiteren Zufallsausgang 12' der Anordnung 100 bilden. Auch an diesen weiteren Zufallsausgang 12' kann ein erzeugtes Zufallssignal, insbesondere erzeugte Zufallszahlen, bereitgestellt werden.

[0071] In einem besonders einfachen Ausführungsbeispiel eines erfindungsgemäßen Verfahrens zur Erzeugung eines Zufallssignals mit der Anordnung 100 des ersten Ausführungsbeispiels wird ein unmoduliertes, optisches Signal S_o durch die optische Quelle 4, z.B. einem Laser, in den

polarization-multiplexed in-phase/quadrature Modulator 10 eingespeist und an den nested Mach-Zehnder-Modulator 1 weitergeleitet. In der Regel handelt es sich hierbei um ein möglichst starkes optisches Signal S_o. Die Leistung der Quelle 4 wird dabei idealerweise in einem Bereich gewählt, der gemäß den optischen Verlusten durch den Eingangs-Strahlteiler 40, des nested Mach-Zehnder Modulators 1 bzw. 2 sowie eines eventuellen optischen Strahlteilers am nested Mach-Zehnder Ausgang die Monitorphotodiode 5 bzw. 6 nicht sättigt. Zudem soll die Leistung, die an der Monitorphotodiode 5 bzw. 6 auftrifft, unter Einbehaltung der vorherigen Bedingung maximiert werden, um einen maximalen Pegelabstand (und somit Unterscheidbarkeit) zum Verstärkerrauschen sicherzustellen. Typische Leistungspegel, um diese beiden Bedingungen zu gewährleisten, liegen im Bereich von 6 bis 16 dBm.

[0072] Für die Durchführung eines erfindungsgemäßen Verfahrens ist es dabei ausreichend, wenn zumindest ein Anteil S'_o des am optischen Eingang 101 des polarization-multiplexed in-phase/quadrature Modulators 10 einlangenden optischen Signal S_o an den nested Mach-Zehnder-Modulator 1 weitergeleitet wird, wie dies der Fall sein kann, wenn ein Eingangs-Strahlteiler 40 vorgesehen ist. Durch den nested Mach-Zehnder-Modulator 1 wird der Anteil S'_o des am optischen Eingang 101 einlangenden optischen Signals S_o entsprechend dem vorgegebenen Arbeitspunkt moduliert. Obwohl für die Generierung eines Zufallssignal keine ähnlich wie bei der Datenübertragung eingesetzten schnellen Modulation notwendig ist, kann der Arbeitspunkt günstigerweise so definiert werden, dass die zur Monitorphotodiode 5 zugeführte optische Leistung durch den nested Mach-Zehnder-Modulator 1 definiert werden kann. Mit der Einstellung des Arbeitspunktes kann durch die interferometrische Struktur des Mach-Zehnder-Modulators 1, wie in Abbildung 2 erläutert, die Leistung dessen optischen Ausgangs 15 gesteuert werden. Der Mach-Zehnder-Modulator 1 erscheint dadurch als ein variabler optischer Abschwächer.

[0073] Zur Erzeugung eines Zufallssignals wird zumindest ein Anteil $S_{o,M1}$ des vom nested Mach-Zehnder-Modulator 1 bereitgestellten optischen Ausgangssignals an die Monitorphotodiode 5 weitergeleitet und in ein elektrisches Signal $S_{el,D1}$ umgewandelt. Am elektrischen Monitorphotodiodenausgang 52 der Monitorphotodiode 5 liegt somit schließlich ein elektrisches Signal $S_{el,D1}$ an. Dieses elektrische Signal $S_{el,D1}$ der Monitorphotodiode 5 stellt ein Zufallssignal dar, da der inhärent zufällige Charakter des von der optischen Quelle 4 eingespeisten optischen Signals S_o, der durch dessen Quanteneigenschaften bedingt ist, genutzt werden kann. Die Anzahl der in einem Zeitintervall detektierten Photonen und dadurch erzeugten Ladungsträgerpaare und damit der durch die Monitorphotodiode fließende Strom können jeweils als Zufallsvariable mit Poissonverteilung beschrieben werden. Diese Zufälligkeit des Stroms bezeichnet man als Schrotrauschen.

[0074] Somit bildet der elektrische Monitorphotodiodenausgang 52 der Monitorphotodiode 5 einen Zufallsausgang 12 der Anordnung 100.

[0075] Im ersten Ausführungsbeispiel einer erfindungsgemäßen Anordnung 100 in Fig. 1 sind, wie bereits zuvor beschrieben, ein weiterer nested Mach-Zehnder-Modulator 2 und eine weitere Monitorphotodiode 6 vorhanden. In diesem Fall kann ein weiterer Anteil S''_o des am optischen Eingang 101 des polarization-multiplexed in-phase/quadrature Modulators 10 einlangenden optischen Signals S_o an den weiteren nested Mach-Zehnder-Modulator 2 weitergeleitet und von diesem moduliert werden.

[0076] Anschließend wird zumindest ein Anteil $S_{o,M2}$ des vom weiteren nested Mach-Zehnder-Modulator 2 bereitgestellten optischen Ausgangssignals an die weitere Monitorphotodiode 6 weitergeleitet und in ein elektrisches Signal $S_{el,D2}$ umgewandelt. Wie oben schrieben, wird in diesem Fall am elektrischen Monitorphotodiodenausgang 62 der weiteren Monitorphotodiode 6 das elektrische Signal $S_{el,D2}$ als Zufallssignal bereitgestellt. Der elektrische Monitorphotodiodenausgang 62 der weiteren Monitorphotodiode 6 bildet somit im ersten Ausführungsbeispiel einen weiteren Zufallsausgang 12' der Anordnung 100.

ZWEITES AUSFÜHRUNGSBEISPIEL EINER ERFINDUNGSGEMÄßEN ANORDNUNG 100, FIG. 3

[0077] Wie in Fig. 3 ersichtlich ist, umfasst das zweite Ausführungsbeispiel einer erfindungsge-

mäßen Anordnung 100 zusätzlich zu den Komponenten des ersten Ausführungsbeispiels dargestellt in Fig. 1 eine Umwandlungseinheit 7, deren Ausgang den Zufallsausgang 12 der Anordnung 100 bildet. Der elektrische Monitorphotodiodenausgang 52 der Monitorphotodiode 5 und der elektrische Monitorphotodiodenausgang 62 der weiteren Monitorphotodiode 6 sind an die Umwandlungseinheit 7 angeschlossen.

[0078] Eine derartige Umwandlungseinheit kann einen modularen Aufbau aufweisen. Im Folgenden werden anhand der Fig. 3 und Fig. 4 verschiedene Ausführungsbeispiele einer Umwandlungseinheit 7 einer erfindungsgemäßen Anordnung 100 beschrieben:

[0079] So kann die Umwandlungseinheit 7 einen Transimpedanzverstärker 8 umfassen, wie er schematisch in Fig. 4 dargestellt ist. Der Transimpedanzverstärker 8 weist einen ersten elektrischen Transimpendanzverstärker-Eingang 81, einen zweiten elektrischen Transimpendanzverstärker-Eingang 82 und einen elektrischen Transimpedanzverstärker-Ausgang 83 auf. Der elektrische Monitorphotodiodenausgang 52 der Monitorphotodiode 5 ist an den ersten elektrischen Transimpendanzverstärker-Eingang 81 angeschlossen und der elektrische Monitorphotodiodenausgang 62 der weiteren Monitorphotodiode 6 ist an den zweiten elektrischen Transimpendanzverstärker-Eingang 82 angeschlossen. Der Transimpedanzverstärker-Ausgang 83 kann dabei optional den Ausgang der Umwandlungseinheit 7, d.h. den Zufallsausgang 12 der Anordnung 100, bilden.

[0080] Die Umwandlungseinheit 7 kann, wie in Fig. 4, optional zusätzlich auch eine analoge Signalverarbeitungseinheit 70 mit einem elektrischen Eingang 71 und einem elektrischen Ausgang 72 umfassen. Ist eine derartige analoge Signalverarbeitungseinheit 70 vorhanden, ist der elektrische Transimpedanzverstärker-Ausgang 83 an den elektrischen Eingang 71 der analogen Signalverarbeitungseinheit 70 angeschlossenen und der elektrische Ausgang 72 der analogen Signalverarbeitungseinheit 70 kann den Ausgang der Umwandlungseinheit 7, d.h. den Zufallsausgang 12 der Anordnung 100, bilden.

[0081] Die Umwandlungseinheit 7 kann, wie in Fig. 4, optional auch einen Analog-Digital-Wandler 9 umfassen. Ein derartiger Analog-Digital-Wandler 9 weist einen elektrischen Wandlereingang 91 und einen elektrischen Wandlerausgang 92 auf, der den Ausgang der Umwandlungseinheit 7, d.h. den Zufallsausgang 12 der Anordnung 100, bilden kann. Umfasst die Umwandlungseinheit 7 einen derartigen Analog-Digital-Wandler 9, so kann einerseits der elektrische Transimpedanzverstärker-Ausgang 83 unmittelbar an den elektrischen Wandlereingang 91 angeschlossen sein. Andererseits ist es auch möglich, sollte die Umwandlungseinheit 7 eine analoge Signalverarbeitungseinheit 70 umfassen, dass der elektrische Ausgang 72 der analogen Signalverarbeitungseinheit 70 an den elektrischen Wandlereingang 91 angeschlossenen ist.

[0082] Die Umwandlungseinheit 7 kann, wie in Fig. 4, optional zusätzlich auch eine digitale Signalverarbeitungseinheit 11 umfassen. Eine derartige digitale Signalverarbeitungseinheit 11 weist einen elektrischen Signaleingang 111 und einen elektrischen Signalausgang 112 auf, der optional als Ausgang der Umwandlungseinheit 7 dienen und den Zufallsausgang 12 der Anordnung 100 bilden kann. Im Fall, dass eine derartige digitale Signalverarbeitungseinheit 11 vorgesehen ist, kann der elektrische Wandlerausgang 92 an den elektrischen Signaleingang 111 der digitalen Signalverarbeitungseinheit 11 angeschlossen sein.

[0083] Die Umwandlungseinheit 7 kann, wie in Fig. 4, optional zusätzlich auch einen Entropieschätzer 13 umfassen, der aus dem bekannten Verhalten der optischen Komponenten der Anordnung 100 und der elektrischen Komponenten der Anordnung 100 eine Entropie des am elektrischen Wandlerausgang 92 bereitgestellten binären Zufallssignals S_b berechnen und zur Verfügung halten kann. Optional können zusätzlich zur Berücksichtigung des optischen Verhaltens auch Parameter wie die Entropiezahl ε vorgegeben und bei der Berechnung der Entropie berücksichtigt werden. Der Entropieschätzer 13 kann z.B. in die digitale Signalverarbeitungseinheit 11 integriert oder an diese angeschlossen sein.

[0084] Bei den optischen Komponenten, kann es sich, wie zuvor beschrieben, um die optische Quelle 4 und/oder die jeweilige Monitorphotodiode 5, 6 und/oder den polarization-multiplexed in-

phase/quadrature Modulator 10 selbst handeln, während es sich bei den elektrischen Komponenten um die zumindest eine Steuereinheit 3 und/oder den Transimpedanzverstärker 8 und/oder den Analog-Digital-Wandler 9 handeln kann.

[0085] Wie im zweiten Ausführungsbeispiel einer erfindungsgemäßen Anordnung 100, dargestellt in Fig. 3, kann der optische Ausgang 15 des nested Mach-Zehnder-Modulators 1 optional an den Eingang 181 eines internen Strahlteilers 18 geführt sein. Ein erster optischer Ausgang 182 des internen Strahlteilers 18 ist bei der erfindungsgemäßen Anordnung 100 in Fig. 3 an den optischen Monitorphotodiodeneingang 51 der Monitorphotodiode 5 angeschlossen. Dies ist jedoch nicht zwingend erforderlich. Alternativ dazu könnte der optische Ausgang 15 des nested Mach-Zehnder-Modulators 1 auch unmittelbar an den optischen Monitorphotodiodeneingang 51 der Monitorphotodiode 5 angeschlossen sein.

[0086] Wie im zweiten Ausführungsbeispiel in Fig. 3 kann auch der optische Ausgang 22 des weiteren nested Mach-Zehnder-Modulators 2 optional an den Eingang 191 eines weiteren internen Strahlteilers 19 geführt sein. Ein erster optischer Ausgang 192 des weiteren internen Strahlteilers 19 ist an den optischen Monitorphotodiodeneingang 61 der weiteren Monitorphotodiode 6 angeschlossen. Dies ist jedoch nicht zwingend erforderlich. Alternativ dazu könnte der optische Ausgang 22 des weiteren nested Mach-Zehnder- Modulators 2 auch unmittelbar an den optischen Monitorphotodiodeneingang 61 der weiteren Monitorphotodiode 6 angeschlossen sein.

[0087] Beim Ausführungsbeispiel in Fig. 3 wird das optische Signal S_o am Eingang 101 des polarization-multiplexed in-phase/quadrature Modulators 10 am Eingangsstrahlteiler 40 verzweigt bzw. gesplittet, idealerweise genau in einen Verhältnis 50/50, und an den nested Mach-Zehnder-Modulator 1 und den weiteren nested Mach-Zehnder-Modulator 2 weitergeleitet. Die 50/50 Verteilung ist besonders günstig, damit im Falle der Differenzbildung der Gleichspannungsanteil vollständig unterdrückt wird um eine Sättigung der nachfolgenden Stufe zu verhindern. Dementsprechend soll auch der Anteil $S_{o,M1}$ des vom nested Mach-Zehnder-Modulator 1 bereitgestellten optischen Signals, der an die Monitorphotodiode 5 weitergeleitet wird, dem Anteil $S_{o,M2}$ des vom weiteren nested Mach-Zehnder-Modulator 2 bereitgestellten optischen Signals, der an die weitere Monitorphotodiode 6 weitergeleitet wird, entsprechen.

[0088] Da es zu Verlusten im jeweiligen nested Mach-Zehnder-Modulator 1, 2 kommen kann, kann es schwierig zu erreichen sein, dass nach der Verzweigung bzw. Splittung des optischen Signals S_o in einem Verhältnis 50/50, anschließend auch der Anteil $S_{o,M1}$ des vom nested Mach-Zehnder-Modulator 1 bereitgestellten optischen Signals, der an die Monitorphotodiode 5 weitergeleitet wird, dem Anteil $S_{o,M2}$ des vom weiteren nested Mach-Zehnder-Modulator 2 bereitgestellten optischen Signals, der an die weitere Monitorphotodiode 6 weitergeleitet wird, entspricht.

[0089] Weiters kann die Ungenauigkeit z.B. eines Tap-Couplers (z.B. eines internen Strahlteilers vor einer Monitorphotodiode) oder eines anderen Strahlteilers bzw. Splitters, zu einer ungleichen Teilung des optischen Signals bzw. einem Ungleichgewicht der Anteile $S_{o,M1}$, $S_{o,M2}$ des vom jeweiligen nested Mach-Zehnder-Modulator 1, 2 bereitgestellten optischen Signals, der an die Monitorphotodiode 5, 6 weitergeleitet wird, führen. Ein derartiger Tap-Coupler kann z.B. als interner Strahlteiler 18, 19 z.B. am jeweiligen Ausgang 15, 22 des jeweiligen nested Mach-Zehnder-Modulators 1, 2 angeordnet sein und z.B. 10% des optischen Signals, das den nested Mach-Zehnder-Modulator 1, 2 verlässt, zu den Monitorphotodioden 5, 6 abzweigen.

[0090] Weiters kann ein ungenaues Teilerverhältnis bereits am Eingangs-Strahlteiler 40 dazu führen, dass das optische Signal S_o in einem Verhältnis ungleich 50/50 geteilt wird. In diesen Fällen muss eine Kompensation dieser ungleichen Verteilung durchgeführt werden. Dies kann erzielt werden, indem die nested Mach-Zehnder-Modulatoren 1, 2 als variable Abschwächer verwendet werden.

[0091] Dazu werden die Arbeitspunkte der nested Mach-Zehnder-Modulatoren 1, 2 von der Steuereinheit 3 so eingestellt, dass der Gleichanteil der Photodiodenströme, d.h. der elektrischen Signale $S_{el,D1}$, $S_{el,D2}$, an den Monitorphotodiodenausgängen 52, 62 der Monitorphotodioden 5, 6 gleich wird. Die zuvor bereits beschriebene interferometrische Anordnung der nested Mach-Zehn-

der-Modulatoren 1, 2 erlaubt dies, da hier Leistung abgeschwächt werden kann. In der Regel kann aber nicht beliebig viel abgeschwächt bzw. vernichtet werden, da der Gleichanteil der Photodiodenströme groß sein soll. Je höher der Gleichanteil der Photodiodenströme ist, umso höher ist die Varianz des Zufallssignals und damit auch die Generierungsrate der Zufallszahlen. Zudem wird darauf geachtet, dass der hohe Photodiodenstrom keine Sättigung der Monitorphotodiode bewirkt.

[0092] Vorzugsweise wird daher die Leistung an den beiden optischen Ausgängen 15, 22 der nested Mach-Zehnder-Modulatoren 1, 2 maximiert und anschließend der stärkere optische Ausgang 15, 22 der beiden nested Mach-Zehnder-Modulatoren 1, 2 durch eine Abänderung des Arbeitspunktes ein wenig abgeschwächt, um ihn dem geringfügig schwächeren optischen Ausgang 15, 22 anzugleichen. Der Abgleich erfolgt wiederum gemäß der Gleichanteile der Photodiodenströme an den Monitorphotodiodenausgängen 52, 62 der Monitorphotodioden 5, 6, die gleich sein sollen. Je nach Auslegung der nested Mach-Zehnder-Modulatoren 1, 2 kann die jeweilige Monitorphotodiode 5, 6 durch einen internen Strahlteiler 18, 19, z.B. einen Tap-Koppler, der typischerweise 10% zur Monitorphotodiode 5, 6 abzweigt, angespeist werden.

[0093] Optional ist es, wie im ersten Ausführungsbeispiel auch möglich, dass die Monitorphotodioden 5, 6 durch den komplementären Mach-Zehnder-Interferometer-Ausgang des jeweiligen nested Mach-Zehnder-Modulators 1, 2 angespeist werden. Wie zuvor bereits beschrieben, stellt jedes Mach-Zehnder-Interferometer $MZI_{1,a}$, $MZI_{1,b}$ zwei Ausgänge bereit, die komplementär wirken, d.h. ein Ausgang erfährt konstruktive, der andere destruktive Interferenz, wie dies bereits zuvor beschrieben wurde. Im Fall, dass die jeweilige Monitorphotodiode 5, 6 am komplementären Ausgang angeschlossen ist, steht der jeweils andere, optische Ausgang des jeweiligen Mach-Zehnder-Interferometers $MZI_{1,a}$, $MZI_{1,b}$ des jeweiligen nested Mach-Zehnder-Modulators 1, 2 z.B. für Datenübertragung komplementär zum Eingang 51, 61 der jeweiligen Monitorphotodiode 5, 6 zur Verfügung.

[0094] In diesem Fall werden die Arbeitspunkte der nested Mach-Zehnder-Modulatoren 1, 2 so eingestellt, dass am optischen Ausgang des jeweiligen Mach-Zehnder-Interferometer $MZI_{1,a}$, $MZI_{1,b}$ minimale Leistung abgegeben wird, sodass am Monitorphotodiodeneingang 51, 61 der jeweiligen Monitorphotodiode 5, 6 maximale Leistung auftritt, da die beiden Ausgänge der Mach-Zehnder-Interferometer $MZI_{1,a}$, $MZI_{1,b}$ komplementär, also gegenläufig ausgebildet sind.

[0095] Zur Bereitstellung eines verstärkten, analogen Zufallssignals S_{va} werden die an den Monitorphotodiodenausgängen 52, 62 der Monitorphotodiode 5, 6 anliegenden elektrischen Signale $S_{el,D1}$, $S_{el,D2}$ anschließend verknüpft. Der Transimpedanzverstärker 8 bildet dazu im zweiten Ausführungsbeispiel, eine Funktion, z.B. die Differenz, der an den elektrischen Monitorphotodiodenausgängen 52, 62 der Monitorphotodioden 5, 6 anliegenden elektrischen Signale $S_{el,D1}$, $S_{el,D2}$ und verstärkt diese.

[0096] Der Transimpedanzverstärker 8 verstärkt also die Differenz der beiden elektrischen Signale $S_{el,D1}$, $S_{el,D2}$, d.h. die Monitorphotodiodenströme der Monitorphotodioden 5, 6. Da die Gleichanteile der elektrischen Signale $S_{el,D1}$, $S_{el,D2}$ gleich sind, werden die Gleichanteile der beiden elektrischen Signale $S_{el,D1}$, $S_{el,D2}$ bei der Differenzbildung entfernt. Allerdings besitzen die elektrischen Signale $S_{el,D1}$, $S_{el,D2}$ der Monitorphotodioden 5, 6, d.h. deren Monitorphotodiodenströme, auch einen Wechselanteil, der dem Quantenrauschen der optischen Quelle 4, z.B. eines Lasers, entspricht.

[0097] Dieser Wechselanteil wird nun verstärkt und steht nun als verstärktes elektrisches „Quellsignal" zur Zufallszahlengenerierung zur Verfügung. Auf diese Weise wird also ein verstärktes, analoges Zufallssignal S_{va} am Transimpedanzverstärker-Ausgang 83 bereitgestellt. Sofern der Transimpedanzverstärker-Ausgang 83 den Ausgang der Umwandlungseinheit 7 bildet, wird dieses verstärkte, analoge Zufallssignal S_{va} am Zufallsausgang 12 der Anordnung 100 bereitgestellt.

[0098] Im zweiten Ausführungsbeispiel einer erfindungsgemäßen Anordnung 100 wird das verstärkte, analoge Zufallssignal S_{va} dem elektrischen Eingang 71 der analogen Signalverarbeitungseinheit 70 zugeführt.

[0099] Diese analoge Signalverarbeitungseinheit 70 dient dazu, die Signalqualität des verstärkten, analogen Zufallssignals S_{va}, z.B. vor einer etwaigen Digitalisierung, noch weiter zu verbessern. Dazu kann die analoge Signalverarbeitungseinheit 70 das am Transimpedanzverstärker-Ausgang 83 bereitgestellte verstärkte, analoge Zufallssignal S_{va} z.B. filtern. Auf diese Weise können z.B. ungewollte Störungen oder allfällige Artefakte des I/Q-Transmitters wie Pilottöne, die für den Datenbetrieb benötigt werden, herausgefiltert werden. Derartige spektralen Komponenten würden etwa die effektive Zahl an Bits, mit welcher die Digitalisierung des Rauschsignals erfolgen kann, vermindern, da durch die im Allgemeinen starken Störsignale der Aussteuerbereich verringert und folglich das im Allgemeinen schwächere Rauschsignal nur mit geringerer Auflösung digitalisiert wird.

[00100] Sofern der elektrische Ausgang 72 der analogen Signalverarbeitungseinheit 70 den Ausgang der Umwandlungseinheit 7, d.h. den Zufallsausgang 12 der Anordnung 100 bildet, wird dieses gefilterte verstärkte, analoge Zufallssignal S'_{va} am Zufallsausgang 12 bereitgestellt.

[00101] Im zweiten Ausführungsbeispiel, dargestellt in Fig. 3 und Fig. 4, umfasst die Umwandlungseinheit 7 eine derartige analoge Signalverarbeitungseinheit 70 und das gefilterte verstärkte, analoge Zufallssignal S'_{va} wird dem Wandlereingang 91 des Analog-Digital-Wandlers 9 zugeführt. Sofern die Umwandlungseinheit 7 keine derartige analoge Signalverarbeitungseinheit 70 umfasst, wird das verstärkte, analoge Zufallssignal S_{va} des Transimpedanzverstärkers 8 ohne Filterung unmittelbar dem Wandlereingang 91 des Analog-Digital-Wandlers 9 zugeführt.

[00102] Der Analog-Digital-Wandlers 9 wandelt das elektrische analoge Quellsignal, d.h. das verstärkte, analoge Zufallssignal S_{va}, das gegebenenfalls auch gefiltert sein kann, in ein digitales, binäres Zufallssignal S_b um. Dieses binäre Zufallssignal S_b stellt der Analog- Digital-Wandlers 9 am elektrischen Wandlerausgang 92 bereit. Falls der elektrische Wandlerausgang 92 den Zufallsausgang 12 der Umwandlungseinheit 7 bildet, wird dieses binäre Zufallssignal S_b am Zufallsausgang 12 der Anordnung 100 bereitgestellt.

[00103] Die Auflösung des Analog-Digital-Wandlers 9 beträgt vorzugsweise mindestens 1 bit. Der genaue Wert der Auflösung (bit am ADC Ausgang) kann an die gewünschte Rate an Zufallszahlen angepasst werden. Alternative kann die Auflösung sehr niedrig gewählt werden, um Komplexität zu reduzieren. Dies kann im Extremfall zu einer einfachen Komparator-Lösung mit 1 bit Auflösung führen. Der Wandlerausgang 92 kann die digitalen Daten auf einer Leitung seriell ausgeben oder auf mehreren Leitungen parallel.

[00104] Der Analog-Digital-Wandler 9 kann vorteilhafterweise über eine Abtasteinheit - Sample & Hold - verfügen, um das analoge Quellsignal für kurze Zeit konstant zu halten. Die Zeitpunkte können von einer Wandler-Steuereinheit definiert werden, die im Analog-Digital-Wandler 9 integriert sein kann. Eine Möglichkeit besteht darin, dass die Wandler-Steuereinheit ein periodisches Signal erzeugt, damit das gefilterte, verstärkte, analoge Zufallssignal S'_{va} periodisch abgetastet wird. Die Wandler-Steuereinheit kann von der Entropieschätzung instruiert werden. Die Entropieschätzung kann die Abtastperiode (bzw. Abtastfrequenz) z.B. in Abhängigkeit vom gefilterten Fourierspektrum des Rauschsignals so vorgeben, dass die geschätzte Entropie maximiert wird. Das Ausgangssignal der Abtasteinheit wird dem Quantisierer des Analog-Digital-Wandlers 9 zugeführt. Da ein Analog-Digital-Wandler keine sofortige Wandlung durchführen kann, sollte der Eingabewert während der Zeit, in der der Wandler eine Wandlung durchführt, idealerweise konstant gehalten werden (als Konvertierungszeit bezeichnet). Eine als Abtasteinheit bezeichnete Eingangsschaltung führt diese Aufgabe aus. Danach wird dieses kurzzeitig konstante Signal dem Quantisierer des Wandlers zugeführt, damit die eigentliche Wandlung erfolgen kann.

[00105] In Fig. 4 ist der elektrische Wandlerausgang 92 an die digitale Signalverarbeitungseinheit 11 angeschlossen. Die digitale Signalverarbeitungseinheit 11 erstellt aus dem am elektrische Wandlerausgang 92 bereitgestellten binären Zufallssignal S_b ein binäres Zufallssignal S_{EE}, insbesondere eine Zufallszahl, mit verbesserten statistischen Eigenschaften, hier konkret erhöhter Entropie pro bit. „Erhöhte Entropie pro bit" ist hier so zu verstehen, dass das binäre Zufallssignal S_{EE}, das von der digitalen Signalverarbeitungseinheit 11 erzeugt und an ihrem elektrischen Signalausgang 112 bereitgestellt wird, im Vergleich zum binären Zufallssignal S_b des Analog-Digital-Wand-

lers 9 erhöhte Entropie pro bit aufweist. Dies kann auf verschiedene Weise erzielt werden:

[00106] Wie zuvor bereits erwähnt, verfügt die digitale Signalverarbeitungseinheit 11 im zweiten Ausführungsbeispiel über einen Entropieschätzer 13. Der Entropieschätzer errechnet aus dem bekannten Verhalten der optischen Komponenten der Anordnung 100 und der elektrischen Komponenten der Anordnung 100 eine Entropie des am elektrischen Wandlerausgang 92 bereitgestellten binären Zufallssignals S_b. Hierbei kann der Entropieschätzer 13 z.B. die Shannon-Entropie, eine Renyi-Entropie, oder die Min- Entropie wie in Miguel Herrero-Collantes, Juan Carlos Garcia-Escartin, "Quantum Random Number Generators", Reviews of Modern Physics 89, 015004 (2017), oder Tomamichel, Marco, "Quantum Information Processing with Finite Resources", Springer, Mathematical Foundations, ISBN 978-3-319-21891-5, beschrieben, oder auch eine bedingte Entropie, wie die bedingte Shannon-Entropie, eine bedingte Renyi-Entropie oder eine bedingte Min-Entropie (wobei die Bedingung jeweils z.B. die vorhandene Information eines möglichen Angreifers, z.B. betreffend Verstärker-Eigenschaften sein kann), wie ebenfalls in Miguel Herrero-Collantes, Juan Carlos Garcia-Escartin, "Quantum Random Number Generators", Reviews of Modern Physics 89, 015004 (2017), oder Tomamichel, Marco, "Quantum Information Processing with Finite Resources", Springer, Mathematical Foundations, ISBN 978-3-319-21891-5, beschrieben, des am elektrischen Wandlerausgang 92 bereitgestellten binären Zufallssignals S_b berechnen und für die digitale Signalverarbeitungseinheit 11 zur Verfügung zu halten.

[00107] Optional können zusätzlich zur Berücksichtigung des optischen Verhaltens auch Parameter wie ε, das den statistischen Abstand der erzeugten Zufallszahlen von der Gleichverteilung charakterisiert, vorgegeben und bei der Berechnung der Entropie berücksichtigt werden. So kann der Entropieschätzer 13 z.B. eine parametrisierte Entropie, wie die ε-smooth Min-Entropie (siehe Miguel Herrero-Collantes, Juan Carlos Garcia-Escartin, "Quantum Random Number Generators", Reviews of Modern Physics 89, 015004 (2017) , oder Tomamichel, Marco, "Quantum Information Processing with Finite Resources", Springer, Mathematical Foundations, ISBN 978-3-319-21891-5), oder eine parametrisierte bedingte Entropie, insbesondere die bedingte ε-smooth Min-Entropie (siehe ebenfalls Miguel Herrero-Collantes, Juan Carlos Garcia-Escartin, "Quantum Random Number Generators", Reviews of Modern Physics 89, 015004 (2017), oder Tomamichel, Marco, "Quantum Information Processing with Finite Resources", Springer, Mathematical Foundations, ISBN 978-3-319-21891-5), des am elektrischen Wandlerausgang 92 bereitgestellten binären Zufallssignals S_b berechnen und für die digitale Signalverarbeitungseinheit 11 zur Verfügung zu halten.

[00108] Verfügt der Analog-Digital-Wandler 9 über eine Abtasteinheit und eine Wandler-Steuereinheit, benötigt der Entropieschätzer 13 zusätzlich Informationen darüber, welches Signal die Wandler-Steuereinheit erzeugt, um die Entropie des am elektrischen Wandlerausgang 92 bereitgestellten binären Zufallssignals S_b berechnen zu können.

[00109] Steht ein derartiger Entropieschätzer 13 zur Verfügung, zieht die digitale Signalverarbeitungseinheit 11 die vom Entropieschätzer 13 bestimmte Entropie heran, um eine Zufallsvariable mit definierter Entropie pro bit bzw. mit definiertem Minimumwert für eine Entropie pro bit bzw. Block oder mit definiertem Minimumwert für den statistischen Abstand zur Gleichverteilung oder mit definiertem Minimumwert für den statistischen Abstand zu einer anderen gewünschten Wahrscheinlichkeitsverteilung bereitzustellen. Die digitale Signalverarbeitungseinheit 11 kann einerseits das Ausgangssignal des Analog-Digital-Wandlers 9, d.h. das am elektrischen Wandlerausgang 92 bereitgestellte binäre Zufallssignal S_b, und das Ausgangssignal des Entropieschätzers 13 zu einem Strom von digitalen Zufallszahlen mit garantierter Entropie verarbeiten. Die digitale Signalverarbeitungseinheit 11 kann hierzu bekannte Zufallszahlextraktionsverfahren wie z.B. einen von Neumann Extraktor (beschreiben z.B. in , John von Neumann, "Various Techniques Used in Connection With Random Digits" J. Res. Nat. Bur. Stand. Appl. Math. Series 3, 36-38 (1951)) verwenden.

[00110] Die zugrundeliegende Zufallsvariable, der so bestimmten Zufallszahl, hat vorzugsweise eine Entropie möglichst nahe an 1 bit pro bit bzw. ist deren Verteilung statistisch möglichst nahe an der Gleichverteilung oder einer anderen gewünschten Verteilung. Dies ist notwendig damit die

Zufallszahl in der Kryptographie und überall dort wo eine konkrete Verteilung benötigt wird, eingesetzt werden kann.

[00111] Die Zufallszahl stellt die digitale Signalverarbeitungseinheit 11 schließlich an ihrem elektrischen Signalausgang 112, im zweiten Ausführungsbeispiel ist dies der Zufallsausgang 12 der Anordnung 100, als Zufallszahl bereit.

[00112] Optional ist es auch möglich, dass zusätzlich einmalig eine Zufallszahl, die der digitalen Signalverarbeitungseinheit 11 bereitgestellt oder in der digitalen Signalverarbeitungseinheit 11 vorab gespeichert wird, für das Zufallszahlextraktionsverfahren herangezogen wird. Dies kann der Fall sein, wenn die digitale Signalverarbeitungseinheit 11 Universal Hashing (z.B. Toeplitz Hashing) (Universal Hashing beschrieben z.B. in Carter, Larry; Wegman, Mark N., "Universal Classes of Hash Functions". Journal of Computer and System Sciences. 18 (2), 143-154 (1979).. Toeplitz hashing beschreiben z.B. in Mansour, Y., N. Nisan and P. Tiwari, "The computational complexity of universal hashing", Theoretical Computer Science 107, 121133 (1993)) für die Erstellung von digitalen Zufallszahlen mit garantierter Entropie heranzieht. Denkbar ist auch, dass diese Zufallszahl über eine externe Schnittstelle bereitgestellt wird.

DRITTES AUSFÜHRUNGSBEISPIEL EINER ERFINDUNGSGEMÄßEN ANORDNUNG 100

[00113] Im Folgenden wird ein besonders einfach aufgebautes drittes Ausführungsbeispiel einer erfindungsgemäßen Anordnung 100 beschrieben. Im dritten Ausführungsbeispiel weist der polarization-multiplexed in-phase/quadrature Modulator 10 nur einen einzelnen nested Mach-Zehnder-Modulator 1 auf.

[00114] Der optische Eingang 14 des nested Mach-Zehnder-Modulators 1 ist direkt dem optischen Modulatoreingang 101 nachgeschaltet. Die optische Quelle 4 kann dabei beispielsweise unmittelbar auf den optischen Eingang 14 des nested Mach-Zehnder-Modulators 1 gerichtet, bzw. an diesen geführt sein. In diesem Fall wird das optische Signal S_o also ohne gesplittet bzw. verzweigt zu werden, an den optischen Eingang 14 des nested Mach-Zehnder-Modulators 1 geleitet.

[00115] Über den elektrischen Eingang 16 des nested Mach-Zehnder-Modulators 1 werden, wie im ersten und zweiten Ausführungsbeispiel einer erfindungsgemäßen Anordnung 100, von einer Steuereinheit 3 die elektrischen Signale vorgegeben, mit denen der Arbeitspunkt des nested Mach-Zehnder-Modulators 1 eingestellt wird.

[00116] Eine Monitorphotodiode 5 ist dem polarization-multiplexed in-phase/quadrature Modulator 10 nachgeschaltet. Die Monitorphotodiode 5 kann hier direkt dem optischen Ausgang 15 des nested Mach-Zehnder-Modulators 1 nachgeschaltet sein, oder über einen internen Strahlteiler 18 dem optischen Ausgang 15 des nested Mach-Zehnder-Modulators 1 nachgeschaltet sein. Optional ist es auch möglich, dass die Monitorphotodiode 5 auch einem zum Datenausgang des jeweiligen Mach-Zehnder-Interferometers $MZI_{1,a}$, $MZI_{1,b}$ komplementären Ausgang angeschlossen ist, wie dies schematisch in Fig. 1 angedeutet ist.

[00117] Wie zuvor bereits beschrieben, weist die Monitorphotodiode 5 einen elektrischen Monitorphotodiodenausgang 52 auf, der einen Zufallsausgang 12 der Anordnung 100 bildet. An diesem Zufallsausgang 12 wird ein erzeugtes Zufallssignal, insbesondere erzeugte Zufallszahlen, bereitgestellt.

[00118] Im einfachsten Ausführungsbeispiel eines erfindungsgemäßen Verfahrens zur Erzeugung eines Zufallssignals mit der Anordnung 100 des ersten Ausführungsbeispiels wird ein unmoduliertes, optisches Signal S_o durch die optische Quelle 4, z.B. einem Laser, in den polarization-multiplexed in-phase/quadrature Modulator 10 eingespeist und an den nested Mach-Zehnder-Modulator 1 weitergeleitet. Durch den nested Mach-Zehnder-Modulator 1 wird das optische Signal S_o entsprechend dem vorgegebenen Arbeitspunkt moduliert.

[00119] Wie bereits zuvor beschrieben, wird zur Erzeugung eines Zufallssignals zumindest ein Anteil $S_{o,M1}$ des vom nested Mach-Zehnder-Modulator 1 bereitgestellten optischen Ausgangssignals an die Monitorphotodiode 5 weitergeleitet und in ein elektrisches Signal $S_{el,D1}$ umgewandelt. Am elektrischen Monitorphotodiodenausgang 52 der Monitorphotodiode 5 liegt somit schließlich

ein elektrisches Signal $S_{el,D1}$ an. Dieses elektrische Signal $S_{el,D1}$ stellt ein Zufallssignal dar, aufgrund des inhärent zufälligen Charakters des von der optischen Quelle 4 eingespeisten optischen Signals S_o. Somit bildet der elektrische Monitorphotodiodenausgang 52 der Monitorphotodiode 5 einen Zufallsausgang 12 der Anordnung 100.

GLEICHZEITIGES ERZEUGEN EINES ZUFALLSSIGNALS UND SENDEN VON DATEN:

[00120] Wie bereits zuvor erwähnt, ist es vorteilhafterweise möglich, dass eine Monitorphotodiode 5, 6 durch einen, zum Datenausgang des jeweiligen Mach-Zehnder-Interferometers $MZI_{1,a}$, $MZI_{1,b}$ komplementären, Mach-Zehnder-Interferometer-Ausgang des jeweiligen nested Mach-Zehnder-Modulators 1, 2 angespeist werden kann, wie bereits zuvor beschrieben wurde. Wie zuvor bereits beschrieben, stellt jedes Mach-Zehnder-Interferometer $MZI_{1,a}$, $MZI_{1,b}$ zwei Ausgänge bereit, die komplementär wirken, d.h. ein Ausgang erfährt konstruktive, der andere destruktive Interferenz. Im Fall, dass die jeweilige Monitorphotodiode 5, 6 am komplementären Ausgang angeschlossen ist, steht der optische Ausgang 15, 22 des jeweiligen nested Mach-Zehnder-Modulators 1, 2 z.B. für Datenübertragung komplementär zum Eingang 51, 61 der jeweiligen Monitorphotodiode 5, 6 zur Verfügung.

[00121] So können einerseits abwechselnd Daten über den Datenausgang 102 des polarization-multiplexed in-phase/quadrature Modulators 10 übertragen und Zufallszahlen generiert und am Zufallsausgang 12 bereitgestellt werden. Der Datenausgang 102 des polarization-multiplexed in-phase/quadrature Modulators 10 ist dabei den Datenausgängen der nested Mach-Zehnder-Modulatoren 1, 2 nachgeschaltet, wie dies in Fig. 3 ersichtlich ist.

[00122] Der polarization-multiplexed in-phase/quadrature Modulator 10 kann dazu zwei Betriebszustände aufweisen, nämlich einen ersten Betriebszustand, in dem ein Datensignal über den optischen Datenausgang 102 des polarization-multiplexed in-phase/quadrature Modulators 10 übertragen wird und einen zweiten Betriebszustand, in dem ein Zufallssignal, insbesondere Zufallszahlen, wie zuvor beschrieben, erzeugt werden. Zwischen den beiden Betriebszuständen kann gewechselt werden, indem der Arbeitspunkt des polarization-multiplexed in-phase/quadrature Modulators 10 geändert wird. Dies erfolgt in einfachster Form gemäß einem Zeitmultiplex, d.h., die zwei Arbeitspunkteinstellungen wechseln sich zeitlich gemäß einer vorgegebener zeitlichen Folge ab. Diese Folge kann gemäß dem Duty Cycle entweder die Datenübertragung oder die Generierung von Zufallszahlen zeitlich bevorzugen. Das Wechseln zwischen den Arbeitspunkteinstellungen erfolgt dabei durch ein geeignetes elektrisches Ansteuern an den elektrischen Eingängen 16, 23 der nested Mach-Zehnder-Modulatoren 1,2.

[00123] Optional können die beiden Betriebszustände auch gleichzeitig genutzt werden, d.h. gleichzeitig Daten übertragen und Zufallszahlen generiert werden. Dazu wird der Frequenzbereich des polarization-multiplexed in-phase/quadrature Modulators 10 vorteilhafterweise so aufgeteilt wird, sodass der Frequenzbereich des Datensignals und der Frequenzbereich des zumindest einen Zufallssignals, insbesondere der Zufallszahlen, einander nicht überlappen. So kann zum Beispiel der niedrige Frequenzbereich unterhalb des typischen Low-Frequency Cut-Offs der Datensignale (im Bereich von z.B. 0 bis 100 kHz) für die Generierung von Zufallszahlen dienen, während die hohen Frequenzen (von 100 kHz bis 25 GHz) der Datenübertragung dienen. Auf diese Weise kann ein Übersprechen zwischen den beiden Signalen unterdrückt werden. Dies kann zum Beispiel durch passive (Einfügen eines Filters) and aktive Filterung (Frequenzgang eines Verstärkers) erreicht werden.

Patentansprüche

1. Anordnung (100) zur Erzeugung eines Zufallssignals umfassend
   - eine optische Quelle (4), insbesondere einen Laser,
   - einen polarization-multiplexed in-phase/quadrature Modulator (10), der folgende Bestandteile umfasst:
     - einen optischen Modulatoreingang (101), an den die optische Quelle (4) angeschlossen ist,
     - zumindest einen nested Mach-Zehnder-Modulator (1), wobei der zumindest eine nested Mach-Zehnder-Modulator (1) dem optischen Modulatoreingang (101) nachgeschaltet ist und
       wobei der zumindest eine nested Mach-Zehnder-Modulator (1) einen optischen Ausgang (15) und zumindest einen elektrischen Eingang (16) zur Vorgabe des Realteils und/oder des Imaginärteils eines optischen Signals aufweist,
   - eine Steuereinheit (3), die an den elektrischen Eingang (16) des nested Mach- Zehnder-Modulators (1) angeschlossen ist, wobei die Steuereinheit (3) dazu ausgebildet ist, zumindest einen Arbeitspunkt des polarization-multiplexed in-phase/quadrature Modulators (100) vorzugeben,

   dadurch gekennzeichnet,
   dass zumindest eine Monitorphotodiode (5) dem polarization-multiplexed in-phase/quadrature Modulator (10) nachgeschaltet ist, wobei die Monitorphotodiode (5) dem optischen Ausgang (15) des nested Mach-Zehnder-Modulators (1) nachgeschaltet ist und einen elektrischen Monitorphotodiodenausgang (52) aufweist, sodass ein vom nested Mach-Zehnder-Modulator (1) bereitgestelltes optisches Signal in ein elektrisches Signal umwandelbar ist, und
   dass der Monitorphotodiodenausgang (52) der Monitorphotodiode (5) einen Zufallsausgang (12) der Anordnung (100) zur Bereitstellung eines erzeugten Zufallssignals, insbesondere erzeugter Zufallszahlen, bildet.

2. Anordnung (100) nach Anspruch 1, **dadurch gekennzeichnet**,
   - dass der polarization-multiplexed in-phase/quadrature Modulator (10) einen Eingangs-Strahlteiler (17) aufweist, wobei der optische Modulatoreingang (101) an den Eingang (171) des Eingangs-Strahlteilers (17) geführt ist, und wobei ein erster Ausgang (172) des Eingangs-Strahlteilers (40) an den optischen Eingang (14) des nested Mach-Zehnder-Modulators (1) geführt ist und
   - dass die Anordnung einen weiteren nested Mach-Zehnder-Modulator (2) umfasst, wobei ein zweiter Ausgang (173) des Eingangs-Strahlteilers (40) an den optischen Eingang (21) des weiteren nested Mach-Zehnder-Modulator (2) geführt ist und wobei der weitere nested Mach-Zehnder-Modulator (2) einen optischen Ausgang (22) und zumindest einen elektrischen Eingang (23) zur Vorgabe des Realteils und/oder des Imaginärteils eines optischen Signals aufweist,
   dass die Steuereinheit (3), gegebenenfalls eine weitere Steuereinheit, an den elektrischen Eingang (23) des weiteren nested Mach-Zehnder-Modulators (2) angeschlossen ist, dass dem polarization-multiplexed in-phase/quadrature Modulator (10) zumindest eine weitere Monitorphotodiode (6) nachgeschaltet ist, wobei die weitere Monitorphotodiode (6) dem optischen Ausgang (22) des weiteren nested Mach-Zehnder-Modulators (2) nachgeschaltet ist und einen elektrischen Monitorphotodiodenausgang (62) aufweist, sodass ein vom weiteren nested Mach-Zehnder-Modulator (2) bereitgestelltes optisches Signal in ein elektrisches Signal umwandelbar ist, und
   dass der Monitorphotodiodenausgang (62) der weiteren Monitorphotodiode (6) einen Zufallsausgang (12') der Anordnung (100) zur Bereitstellung eines erzeugten Zufallssignals, insbesondere erzeugter Zufallszahlen, bildet.

3. Anordnung (100) nach Anspruch 2, **dadurch gekennzeichnet**, dass die Steuereinheit (3), und/oder gegebenenfalls die weitere Steuereinheit, dazu ausgebildet ist, die Arbeitspunkte des nested Mach-Zehnder-Modulators (1) und des weiteren nested Mach-Zehnder-Modula-

tors (2) derart vorzugeben, dass der Gleichanteil des Photodiodenstroms der Monitorphotodiode (5) und der weiteren Monitorphotodiode (6) gleich ist.

4. Anordnung (100) nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet**,
- dass die Anordnung (100) einen internen Strahlteiler (18) umfasst, wobei ein erster optischer Ausgang (182) des internen Strahlteilers (18) an den optischen Monitorphotodiodeneingang (51) der Monitorphotodiode (5) angeschlossen ist und/oder
- dass die Anordnung (100) einen weiteren internen Strahlteiler (19) umfasst, wobei ein erster optischer Ausgang (192) des weiteren internen Strahlteilers (19) an den optischen Monitorphotodiodeneingang (61) der weiteren Monitorphotodiode (6) angeschlossen ist.

5. Anordnung nach einem der Ansprüche 2 bis 4, **dadurch gekennzeichnet**, dass der elektrische Monitorphotodiodenausgang (52) der Monitorphotodiode (5) und der elektrische Monitorphotodiodenausgang (62) der weiteren Monitorphotodiode (6) an eine Umwandlungseinheit (7) angeschlossen sind, wobei der Ausgang der Umwandlungseinheit (7) den Zufallsausgang (12) der Anordnung (100) bildet.

6. Anordnung nach Anspruch 5, **dadurch gekennzeichnet**, dass die Umwandlungseinheit (7) einen Transimpedanzverstärker (8) umfasst,
wobei der Transimpedanzverstärker (8) einen ersten elektrischen Transimpendanzverstärker-Eingang (81), einen zweiten elektrischen Transimpendanzverstärker-Eingang (82) und einen elektrischen Transimpedanzverstärker-Ausgang (83) aufweist,
wobei der elektrische Monitorphotodiodenausgang (52) der Monitorphotodiode (5) an den ersten elektrischen Transimpendanzverstärker-Eingang (81) angeschlossen ist und wobei der elektrische Monitorphotodiodenausgang (62) der weiteren Monitorphotodiode (6) an den zweiten elektrischen Transimpendanzverstärker-Eingang (82) angeschlossen ist.

7. Anordnung nach Anspruch 6, **dadurch gekennzeichnet**, dass der Transimpedanzverstärker (8) dazu ausgebildet ist, eine Funktion der an den elektrischen Monitorphotodiodenausgängen (52, 62) der Monitorphotodioden (5, 6) anliegenden elektrischen Signale, insbesondere der durch die elektrischen Monitorphotodiodenausgängen (52, 62) der Monitorphotodioden (5, 6) fließenden Ströme, zu bilden und zu verstärken, und derart ein verstärktes, analoges Zufallssignal am Transimpedanzverstärker-Ausgang (83) bereitzustellen,
wobei insbesondere vorgesehen ist, dass der Transimpedanzverstärker-Ausgang (83) den Ausgang der Umwandlungseinheit (7) bildet.

8. Anordnung nach einem der Ansprüche 6 oder 7, **dadurch gekennzeichnet**, dass der Transimpedanzverstärker (8) dazu ausgebildet ist, die Differenz der an den elektrischen Monitorphotodiodenausgängen (52, 62) der Monitorphotodioden (5, 6) anliegenden elektrischen Signale, insbesondere der durch die elektrischen Monitorphotodiodenausgängen (52, 62) der Monitorphotodioden (5, 6) fließenden Ströme, zu bilden.

9. Anordnung nach einem der Ansprüche 5 bis 8, **dadurch gekennzeichnet**, dass die Umwandlungseinheit (7) eine analoge Signalverarbeitungseinheit (70) umfasst, wobei die analoge Signalverarbeitungseinheit (70) einen elektrischen Eingang (71) und einen elektrischen Ausgang (72) aufweist und
wobei der elektrische Transimpedanzverstärker-Ausgang (83) an den elektrischen Eingang (71) der analogen Signalverarbeitungseinheit (70) angeschlossenen ist,
wobei die analoge Signalverarbeitungseinheit (70) dazu ausgebildet ist, das am Transimpedanzverstärker-Ausgang (83) bereitgestellte verstärkte, analoge Zufallssignal zu filtern und am elektrischen Ausgang (72) der analogen Signalverarbeitungseinheit (70) bereitzustellen, wobei insbesondere vorgesehen ist, dass der elektrische Ausgang (72) der analogen Signalverarbeitungseinheit (70) den Ausgang der Umwandlungseinheit (7) bildet.

10. Anordnung nach einem der Ansprüche 5 bis 9, **dadurch gekennzeichnet**, dass die Umwandlungseinheit (7) einen Analog-Digital-Wandler (9) umfasst, wobei der Analog-Digital-Wandler (9) einen elektrischen Wandlereingang (91) und einen elektrischen Wandlerausgang (92) aufweist und

wobei der elektrische Transimpedanzverstärker-Ausgang (83) an den elektrischen Wandlereingang (91) des Analog-Digital-Wandlers (9), insbesondere an den der elektrische Ausgang (72) der analogen Signalverarbeitungseinheit (70), angeschlossenen ist,
wobei der Analog-Digital-Wandler (9) dazu ausgebildet ist, auf Grundlage des am Transimpedanzverstärker-Ausgang (83), insbesondere am elektrischen Ausgang (72) der analogen Signalverarbeitungseinheit (70), bereitgestellten verstärkten, analogen Zufallssignal ein binäres Zufallssignal zu erzeugen und am elektrischen Wandlerausgang (92) bereitzustellen,
wobei insbesondere vorgesehen ist, dass der elektrischen Wandlerausgang (92) den Ausgang der Umwandlungseinheit (7) bildet.

11. Anordnung nach einem der Ansprüche 5 bis 10, **dadurch gekennzeichnet**, dass die Umwandlungseinheit (7) eine digitale Signalverarbeitungseinheit (11) umfasst, wobei die digitale Signalverarbeitungseinheit (11) einen elektrischen Signaleingang (111) und einen elektrischen Signalausgang (112) aufweist und
wobei der elektrische Wandlerausgang (92) an den elektrischen Signaleingang (111) der digitalen Signalverarbeitungseinheit (11) angeschlossen ist, und
wobei die digitale Signalverarbeitungseinheit (11) dazu ausgebildet ist, aus dem am elektrische Wandlerausgang (92) bereitgestellten binären Zufallssignal ein binäres Zufallssignal, insbesondere eine Zufallszahl, mit im Vergleich zur Entropie des vom Analog-Digital-Wandler (9) bereitgestellten binären Zufallssignals verbesserten statistischen Eigenschaften zu erzeugen und an ihrem elektrischen Signalausgang (112) bereitzustellen,
wobei insbesondere vorgesehen ist, dass der elektrischen Signalausgang (112) der digitalen Signalverarbeitungseinheit (11) den Ausgang der Umwandlungseinheit (7) bildet.

12. Anordnung nach Anspruch 11, **dadurch gekennzeichnet**, dass die Umwandlungseinheit (7) einen Entropieschätzer (13) umfasst, wobei der Entropieschätzer (13) dazu ausgebildet ist, aus dem bekannten Verhalten der optischen Komponenten der Anordnung (100), insbesondere der optischen Quelle (4) und/oder des polarization-multiplexed in-phase/quadrature Modulators (10), und der elektrischen Komponenten der Anordnung (100), insbesondere der Steuereinheit (3) und/oder des Transimpedanzverstärkers (8) und/oder des Analog-Digital-Wandlers (9), eine Entropie, insbesondere die Shannon-Entropie oder die Min-Entropie, oder eine bedingte Entropie, insbesondere die bedingte Shannon-Entropie oder die bedingte Min-Entropie, des am elektrischen Wandlerausgang (92) bereitgestellten binären Zufallssignals zu berechnen und zur Verfügung zu halten.

13. Anordnung nach Anspruch 11 oder 12, **dadurch gekennzeichnet**, dass die Umwandlungseinheit (7) einen Entropieschätzer (13) umfasst, wobei der Entropieschätzer (13) dazu ausgebildet ist,
aus dem bekannten Verhalten der optischen Komponenten der Anordnung (200), insbesondere der optischen Quelle (4) und/oder des polarization-multiplexed in-phase/quadrature Modulators (10), und der elektrischen Komponenten der Anordnung (200), insbesondere der Steuereinheit (3) und/oder des Transimpedanzverstärkers (8) und/oder des Analog-Digital-Wandlers (9), sowie anhand vorgegebener Parameter, insbesondere anhand einer vorgegebenen unteren Schranke für eine Entropie, eine parametrisierte Entropie, insbesondere die epsilon-smooth Min-Entropie, oder eine parametrisierte bedingte Entropie, insbesondere die bedingte epsilon-smooth Min- Entropie, des am elektrischen Wandlerausgang (92) bereitgestellten binären Zufallssignals zu berechnen und zur Verfügung zu halten.

14. Anordnung nach Anspruch 13, **dadurch gekennzeichnet**, dass die digitale Signalverarbeitungseinheit (11) dazu ausgebildet ist, die vom Entropieschätzer (13) bestimmte Entropie heranzuziehen, um eine Zufallszahl mit definierter Entropie pro bit, insbesondere mit einer Entropie möglichst nahe an 1 bit pro bit, nach einem Zufallszahlenextraktionsverfahren, insbesondere mittels von Neumann-Extraktion, zu erzeugen und an ihrem elektrischen Signalausgang (112) bereitzustellen.

15. Anordnung nach einem der Ansprüche 13 oder 14, **dadurch gekennzeichnet**, dass die digitale Signalverarbeitungseinheit (11) dazu ausgebildet ist, die vom Entropieschätzer (13) bestimmte Entropie sowie eine vorgegebene, insbesondere in der digitalen Signalverarbeitungseinheit (11) hinterlegte, Zufallszahl heranzuziehen, um eine Zufallszahl mit definierter Entropie pro bit, insbesondere mit einer Entropie möglichst nahe an 1 bit pro bit oder mit einer Verteilung die epsilon-nahe an einer Gleichverteilung ist, nach einem Zufallszahlenextraktionsverfahren, insbesondere mittels Universal Hashing und/oder Toeplitz Hashing, zu erzeugen und an ihrem elektrischen Signalausgang (112) bereitzustellen.

16. Verfahren zur Erzeugung eines Zufallssignals mit einer Anordnung (200), insbesondere nach einem der Ansprüche 1 bis 15, umfassend eine optische Quelle (4) und einen polarization-multiplexed in-phase/quadrature Modulator (10),
- wobei ein optisches Signal (S_o) aus der optischen Quelle (4), insbesondere einem Laser, dem optischen Eingang (101) des polarization-multiplexed in-phase/quadrature Modulators (10) zugeführt wird,
- wobei zumindest ein Anteil (S'_o) des am optischen Eingang (101) des polarization-multiplexed in-phase/quadrature Modulator (10) einlangenden optischen Signal (S_o) an einen nested Mach-Zehnder-Modulator (1) des polarization-multiplexed in-phase/quadrature Modulator (10) weitergeleitet wird,
dadurch gekennzeichnet,
- dass zumindest ein Anteil ($S_{o,M1}$) des vom nested Mach-Zehnder-Modulator (1) bereitgestellten optischen Ausgangssignals an eine Monitorphotodiode (5) weitergeleitet wird, und
- dass ein Zufallssignal in Form des am elektrischen Monitorphotodiodenausgang (52) der Monitorphotodiode (5) anliegenden elektrischen Signals ($S_{el,D1}$) bereitgestellt wird.

17. Verfahren nach Anspruch 16, **dadurch gekennzeichnet**,
- dass ein weiterer Anteil (S''_o) des am optischen Eingang (101) des polarization-multiplexed in-phase/quadrature Modulator (10) einlangenden optischen Signal (S_o) an einen weiteren nested Mach-Zehnder-Modulator (2) des polarization-multiplexed in-phase/quadrature Modulators (10) weitergeleitet wird,
- dass zumindest ein Anteil ($S_{o,M2}$) des vom weiteren nested Mach-Zehnder-Modulator (2) bereitgestellten optischen Ausgangssignals an eine weitere Monitorphotodiode (6) weitergeleitet wird, und
- dass ein Zufallssignal in Form des am elektrischen Monitorphotodiodenausgang (62) der weiteren Monitorphotodiode (6) anliegenden elektrischen Signals ($S_{el,D2}$) bereitgestellt wird.

18. Verfahren nach Anspruch 17, **dadurch gekennzeichnet**, dass die Arbeitspunkte der nested Mach-Zehnder-Modulatoren (1, 2) derart vorgegeben werden, dass der Gleichanteil der Photodiodenströme der beiden Monitorphotodioden (5, 6) gleich ist.

19. Verfahren nach Anspruch 18, **dadurch gekennzeichnet**, dass die an den elektrischen Monitorphotodiodenausgängen (52, 62) der Monitorphotodiode (5, 6) anliegenden elektrischen Signale ($S_{el,D1}$, $S_{el,D2}$) verknüpft werden, sodass derart ein verstärktes, analoges Zufallssignal (S_{va}) bereitgestellt wird,
wobei insbesondere vorgesehen ist, dass die Differenz der elektrischen Signale ($S_{el,D1}$, $S_{el,D2}$) gebildet wird.

20. Verfahren nach Anspruch 19, **dadurch gekennzeichnet**, dass das verstärkte, analoge Zufallssignal (S_{va}), gegebenenfalls gefiltert und, in ein binäres Zufallssignal (S_b) umgewandelt wird.

21. Verfahren nach Anspruch 20, **dadurch gekennzeichnet**, dass die Entropie des binären Zufallssignals (S_b) ermittelt wird und dass daraus ein binäres Zufallssignal (S_{EE}) mit verbesserten statistischen Eigenschaften, insbesondere erhöhter Entropie pro bit, vorzugsweise eine Zufallszahl mit erhöhter Entropie, gegebenenfalls unter Einbeziehung einer vorgegebenen Entropiezahl (ε), berechnet wird.

22. Verfahren nach Anspruch 21, **dadurch gekennzeichnet**, dass das binäre Zufallssignal (S_{EE}) mit verbesserten statistischen Eigenschaften, insbesondere erhöhter Entropie pro bit, gegebenenfalls unter Einbeziehung einer vorgegebenen Zufallszahl, nach einem Zufallszahlenextraktionsverfahren, insbesondere mittels von Neumann-Extraktion oder Universal Hashing oder Toeplitz Hashing, berechnet wird.

23. Verfahren nach einem der Ansprüche 16 bis 22, **dadurch gekennzeichnet**, dass der polarization-multiplexed in-phase/quadrature Modulator (10) zwei Betriebszustände aufweist,
    - wobei im ersten Betriebszustand ein Datensignal über den optischen Ausgang (102) des polarization-multiplexed in-phase/quadrature Modulators (10) übertragen wird und
    - wobei im zweiten Betriebszustand zumindest ein Zufallssignal, insbesondere Zufallszahlen, nach einem Verfahren nach einem der Ansprüche 15 bis 21 erzeugt werden und

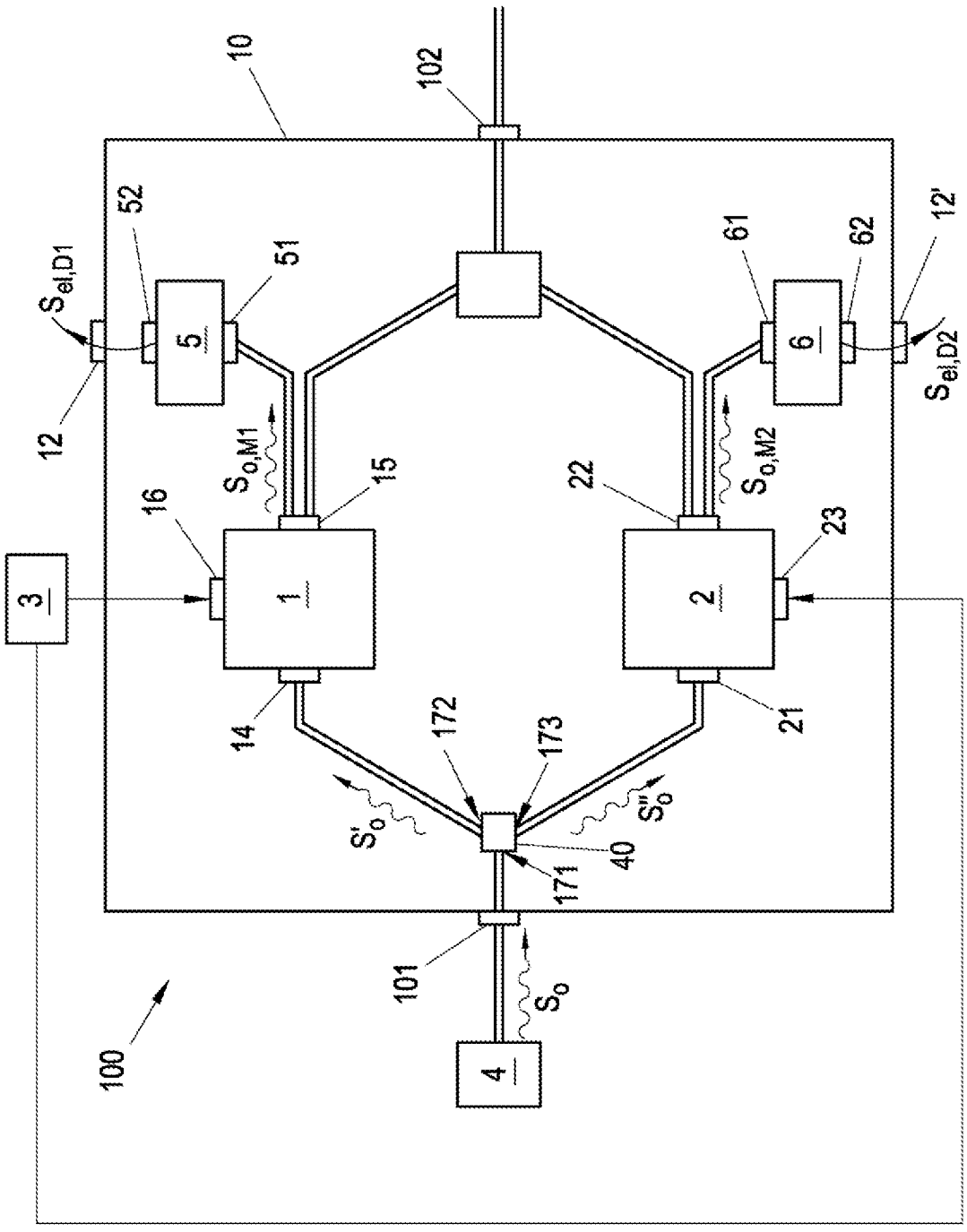
    dass zwischen zwei Betriebszuständen gewechselt wird indem der Arbeitspunkt des polarization-multiplexed in-phase/quadrature Modulators (10) geändert wird.

24. Verfahren nach Anspruch 23, **dadurch gekennzeichnet**, dass die beiden Betriebszustände gleichzeitig genutzt werden, wobei der Frequenzbereich des polarization-multiplexed in-phase/quadrature Modulators (10) derart aufgeteilt wird, sodass der Frequenzbereich des Datensignals und der Frequenzbereich des zumindest einen Zufallssignals, insbesondere der Zufallszahlen, einander nicht überlappen, sodass ein Übersprechen zwischen den beiden Signalen unterdrückt wird.

Hierzu 4 Blatt Zeichnungen

1/4

Fig. 1


10
102
52
51
61
62
12'
$S_{el,D1}$
$S_{el,D2}$
12
5
6
$S_{o,M1}$
$S_{o,M2}$
15
22
16
23
3
1
2
14
172
173
21
S'_o
S''_o
40
171
101
S_o
4
100

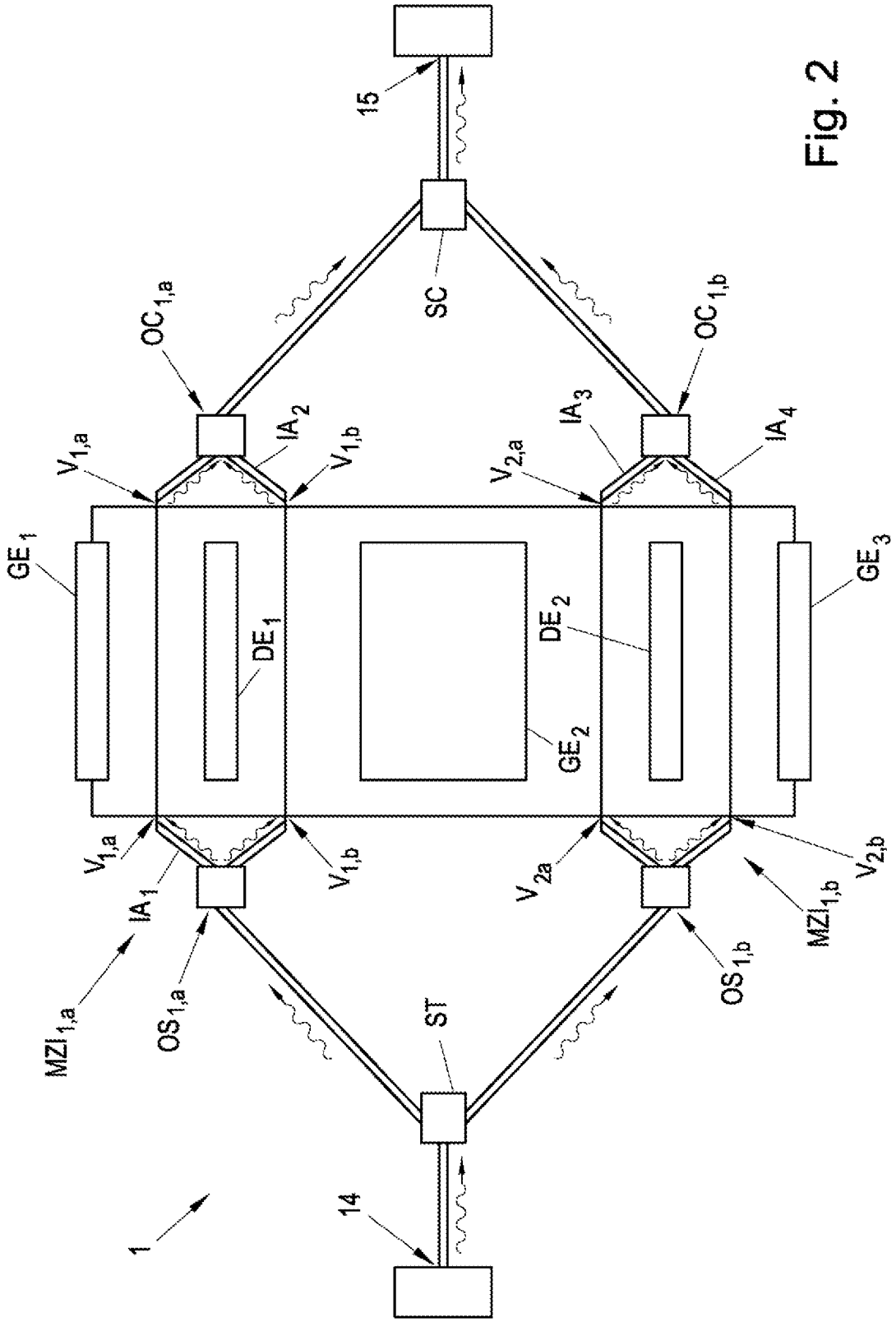

15
SC
OC1,a
OC1,b
IA2
IA3
IA4
V1,a
V1,b
V2,a
GE1
GE3
DE1
DE2
GE2
V1,a
V1,b
V2a
V2,b
IA1
MZI1,a
OS1,a
OS1,b
MZI1,b
ST
14
1

Fig. 2

3/4

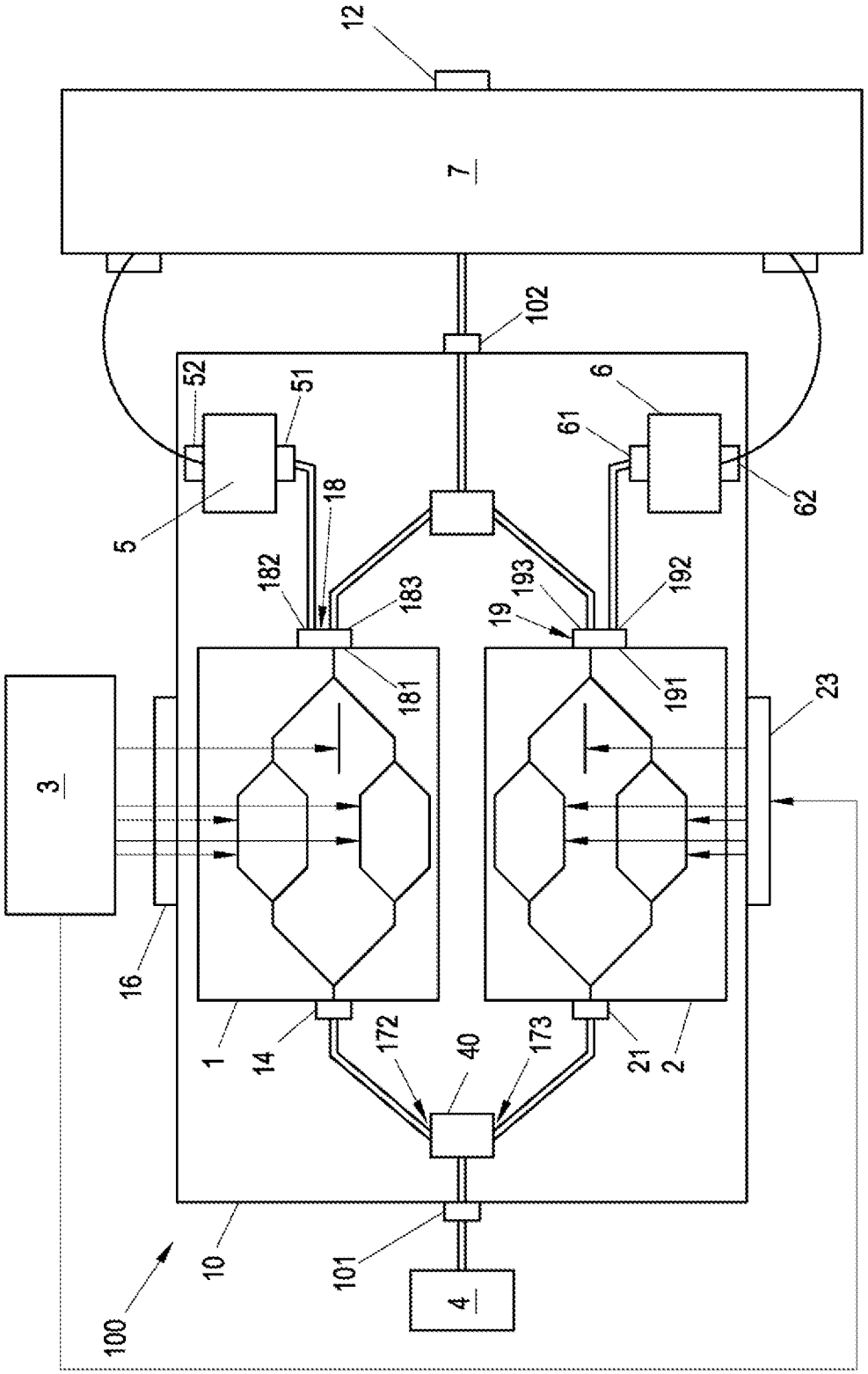

12
7
102
52
51
6
61
62
5
18
182
183
193
192
19
181
191
23
3
16
1
14
172
40
173
21
2
10
101
4
100

Fig. 3

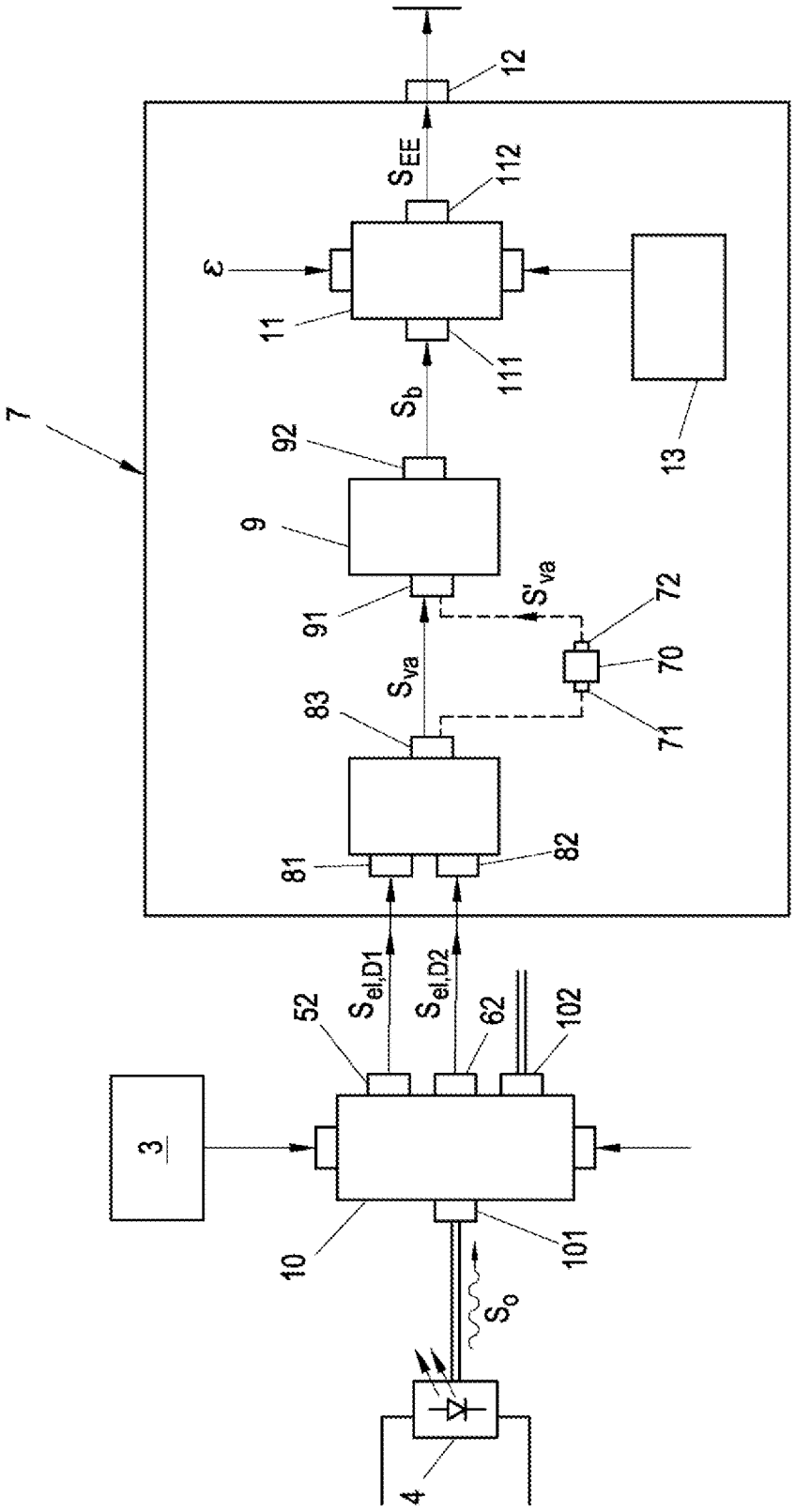

12
S_{EE}
112
ε
11
111
S_b
13
7
92
9
91
S'_{va}
72
70
S_{va}
71
83
81
82
$S_{el,D1}$
$S_{el,D2}$
52
62
102
3
10
101
S_o
4

Fig. 4