(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
27. März 2014 (27.03.2014)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2014/044493 A1

(51) Internationale Patentklassifikation:
G06F 7/58 (2006.01) *H03K 3/84* (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2013/067600

(22) Internationales Anmeldedatum:
26. August 2013 (26.08.2013)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2012 216 892.3
20. September 2012 (20.09.2012) DE

(71) Anmelder: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Wittelsbacherplatz 2, 80333 München (DE).

(72) Erfinder: **DICHTL, Markus**; Jutastr. 14, 80636 München (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

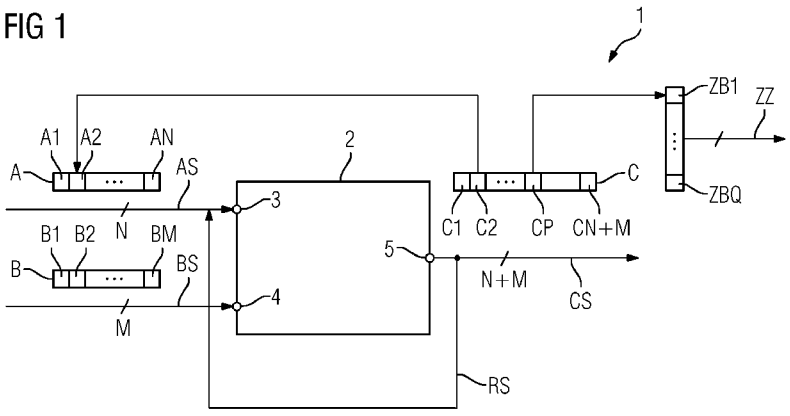
Veröffentlicht:

— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

(54) **Title**: METHOD AND DEVICE FOR GENERATING RANDOM BITS

(54) **Bezeichnung** : VERFAHREN UND VORRICHTUNG ZUM ERZEUGEN VON ZUFALLSBITS

FIG 1



(57) **Abstract**: The invention relates to a method for generating a random bit, having the following steps: providing a combinatorial multiplication device (2) for multiplying two input words (A, B) into an output word (C), comprising at least two inputs (3, 4) and an output (5); generating at least one feedback signal (RS1) dependent on at least one output bit signal (CS1) which can be tapped at the output (5); feeding the feedback signal (RS1) back to an input (4) of the combinatorial multiplication device (2); and tapping at least one output bit signal (CS1) at the output (5) as a random bit signal (ZBS). The invention likewise relates to a corresponding device (1, 100, 101) for generating a random bit, comprising a combinatorial multiplication device (2) and a feedback device (20).

(57) **Zusammenfassung**: Es wird ein Verfahren zum Erzeugen eines Zufallsbits

[Fortsetzung auf der nächsten Seite]

WO 2014/044493 A1

vorgeschlagen, welches umfasst: Bereitstellen einer kombinatorischen Multiplikationseinrichtung (2) zum Multiplizieren von zwei Eingangsworten (A, B) zu einem Ausgangswort (C) mit zumindest zwei Eingängen (3, 4) und einem Ausgang (5); Erzeugen von mindestens einem Rückkopplungssignals (RS1) in Abhängigkeit von mindestens einem Ausgangsbitsignal (CS1), welches an dem Ausgang (5) abgreifbar ist; Rückkoppeln des Rückkopplungssignals (RS1) an einen Eingang (4) der kombinatorischen Multiplikationseinrichtung (29; und Abgreifen von mindestens einem Ausgangsbitsignal (CS1) an dem Ausgang (5) als Zufallsbitsignal (ZBS). Eine entsprechende Vorrichtung (1, 100, 101) zum Erzeugen eines Zufallsbits mit einer kombinatorischen Multiplikationseinrichtung (2) und einer Rückkopplungseinrichtung (20) wird ebenfalls beschrieben.

Beschreibung

Verfahren und Vorrichtung zum Erzeugen von Zufallsbits

Die vorliegende Erfindung betrifft ein Verfahren zum Erzeugen eines Zufallsbits sowie eine Vorrichtung zum Erzeugen eines oder mehrerer Zufallsbits. Es wird zum Beispiel eine Zufallsbitfolge erzeugt, welche als binäre Zufallszahl verwendet wird. Die vorgeschlagenen Vorrichtungen und Verfahren zum Erzeugen von Zufallsbits dienen beispielsweise der Implementierung von Zufallszahlengeneratoren.

In sicherheitsrelevanten Anwendungen, beispielsweise bei asymmetrischen Authentifikationsverfahren, sind Zufallsbitfolgen als binäre Zufallszahlen notwendig. Dabei ist es gewünscht, insbesondere bei mobilen Anwendungen einen möglichst niedrigen Hardwareaufwand zu betreiben. Häufig besteht der Wunsch, mit Hilfe von FPGAs (Field Programmable Gate Array) auf Zufallsbitfolgen zugreifen zu können. FPGAs sind im Anwendungsfeld programmierbare Logikgatteranordnungen, die prinzipiell flexibel eingesetzt und können umprogrammiert werden. Dabei werden Basisblöcke geeignet programmiert bzw. miteinander verschaltet, um gewünschte Funktionen auszuführen.

Die Erzeugung von Zufallsbits ist in der Vergangenheit beispielsweise durch rückgekoppelte Ringoszillatoren oder beispielsweise Fibonacci- oder Galois-Oszillatoren realisiert worden. Nachteilig hat sich dabei erwiesen, dass meist eine nicht ausreichende Zufallsdatenrate realisiert werden kann oder ein hoher Hardwareaufwand betrieben werden muss. Insbesondere bei der Erzeugung von Zufallszahlen in oder mit FPGAs besteht eine Einschränkung durch die von Herstellerseite vorgesehenen Hardwareeinrichtungen. Dedizierte Zufallszahlengeneratoren sind bei den meisten handelsüblichen FPGA-Chips nicht enthalten.

Daher ist eine Aufgabe der vorliegenden Erfindung, ein verbessertes Verfahren und/oder ein verbesserte Vorrichtung zum Erzeugen von Zufallsbits bereitzustellen.

Demgemäß wird ein Verfahren zum Erzeugen eines Zufallsbits vorgeschlagen, welches umfasst:

Bereitstellen einer kombinatorischen Multiplikationseinrichtung zum Multiplizieren von zwei Eingangsworten zu einem Ausgangswort mit mindestens zwei Eingängen und einem Ausgang;

Erzeugen von mindestens einem Rückkopplungssignal in Abhängigkeit von mindestens einem Ausgangsbitsignal, welches an dem Ausgang abgreifbar ist;

Rückkoppeln des Rückkopplungssignals an einen Eingang der kombinatorischen Multiplikationseinrichtung; und

Abgreifen von mindestens einem Ausgangsbitsignal an dem Ausgang als Zufallsbitsignal.

Mit Hilfe einer kombinatorischen Multiplikationseinrichtung, bei der Ausgangs- bzw. Ergebnisbits an Eingangsbits rückgekoppelt werden, entstehen vorzugsweise Oszillationen, die keinen Fixpunkt aufweisen und praktisch zufällige Signalverläufe ergeben. Dabei ist es auch möglich, die rückgekoppelten Bits bzw. die entsprechenden elektrischen Signale zu bearbeiten, wie zum Beispiel logisch zu verknüpfen oder zu invertieren.

Die kombinatorische Multiplikationseinrichtung ist beispielsweise als binäres Multiplikationsrechenwerk in FPGAs enthalten und erfordert somit keine zusätzlichere Ressource. Die durch Rückkopplung entstehenden Schwingungen sind nicht deterministischer Natur, so dass quasi echte Zufallszahlen bzw. Zufallsbits durch periodisches oder regelmäßiges Samplen oder Abtasten eines oder mehrerer Ausgangsbitsignale erzeugt werden.

In Ausführungsformen des Verfahrens werden mehrere Rückkopplungssignale in Abhängigkeit von verschiedenen Ausgangsbitsignalen erzeugt und rückgekoppelt. Es ist beispielsweise

möglich, die verschiedenwertigen Bits des Ausgangswortes entsprechenden Ausgangsbitsignalen als Eingangsbitsignale rückzukoppeln, die verschiedenwertigen Bits der Eingangsworte entsprechen.

In Ausführungsformen des Verfahrens umfasst das Erzeugen des Rückkopplungssignals ein Invertieren des mindestens einen Ausgangssignals. Alternativ können die Ausgangsbitsignale als Rückkopplungssignale auch direkt an Eingangsanschlüsse der Multiplikationseinrichtung geführt werden.

Das Abtasten oder Abgreifen von Ausgangsbitsignalen wird in Ausführungsformen mehrfach durchgeführt. Es ist beispielsweise möglich, periodisch die Eingänge der Multiplikationseinrichtung in wohl definierte Zustände zu versetzen und nach Einstellen einer nicht deterministischen Schwingung eines oder mehrere Zufallsbits zu erfassen.

In Ausführungsformen umfasst das Verfahren und Verknüpfen von Eingangsbitsignalen und/oder des Rückkopplungssignals mit einem Referenzsignal an mindestens einem Eingang der Multiplikationseinrichtung. Das Referenzsignal kann beispielsweise ein Nullsignal sein, welches einem Nullbit entspricht. Durch UND-Verknüpfen aller Eingangsbitsignale für eines der Eingangsworte wird als Ergebnis des Produktes bzw. der Multiplikation eine binäre Null festgelegt. Aus dem entsprechend wohl definierten Startzustand lassen sich dann erneut nicht deterministische Schwingungen erzeugen, um Zufallsbits zu samplen. Beispielsweise ist es möglich, das UND-Verknüpfen und Abgreifen oder Samplen eines Zufallsbits gleichzeitig durchzuführen.

In Ausführungsformen des Verfahrens werden das eine oder mehrere Rückkopplungssignale derart erzeugt und rückgekoppelt, dass das Zufallsbitsignal keinen Fixpunkt erreicht. Beispielsweise kann durch kombinatorische Überlegungen verhindert werden, dass Fixpunkte entstehen. Sind beispielsweise alle Eingangsbits Nullbits, liegt ein Fixpunkt vor. Durch ge-

eignetes Rückkoppeln und Invertieren der Ausgangsbits und Einkoppeln als Eingangsbits von Eingangsworten kann eine Rückkopplung realisiert werden, die keinen Fixpunkt umfasst.

In Ausführungsformen des Verfahrens zum Erzeugen von Zufallsbits haben die Eingänge eine vorgegebene Bitbreite zum Empfangen von Eingangsbitsignalen und der Ausgang eine vorgegebene Bitbreite zum Ausgeben von Ausgangbitsignalen. Das Verfahren umfasst dann ferner Erzeugen eines ersten Rückkopplungsbitsignals in Abhängigkeit von einem Ausgangsbitsignal, welches einem niedrigstwertigen Bit des Ausgangswortes entspricht und Rückkoppeln des ersten Rückkopplungsbitsignals an einen Eingangsanschluss, welcher einem niedrigstwertigen Bit eines Eingangsworts entspricht. Ferner erfolgt ein Erzeugen eines zweiten Rückkopplungsbitsignals in Abhängigkeit von einem Ausgangsbitsignal, welches einem zweitniedrigstwertigen Bit des Ausgangswortes entspricht und Rückkoppeln des zweiten Rückkopplungsbitsignals an einen Eingangsanschluss, welcher einem zweitniedrigstwertigen Bit des anderen Eingangswortes entspricht.

Insbesondere erfolgt vor dem Rückkoppeln jeweils ein Invertieren des Ausgangsbitsignals, welches dem niedrigstwertigen Bit des Ausgangswortes entspricht und ein Invertieren des Ausgangsbitsignals, welches dem zweitniedrigstwertigen Bit des Ausgangswortes entspricht.

Es ist möglich, bei bestimmten Bitbreiten, insbesondere bei einer Bitbreite von fünf Bit für die Eingangsworte, Fixpunkte auszuschließen.

Bei dem Verfahren kann ein Abgreifen von mehreren Ausgangsbitsignalen, welche unterschiedlichen Bits des Ausgangswortes entsprechen, an dem Ausgang als mehrere Zufallsbitsignale erfolgen. Insofern werden die Ausgangsbitsignale, welche unterschiedlichen Bitwertigkeiten des Ausgangs- oder Ergebniswortes entsprechen, als praktisch unabhängige Zufallsbitsignale betrachtet. Es ist auch möglich, potenziell vorliegende sta-

tistische Korrelationen zwischen abgegriffenen Zufallsbits nachzubehandeln, um eine vollständige Zufälligkeit Null- und Eins-Werte zu erzielen. Dadurch kann die Erzeugungsrate der Zufallsbits erhöht werden.

Es ist ferner denkbar, dass in Ausführungsformen des Verfahrens nach dem Abgreifen von dem mindestens einen Ausgangsbitsignal an dem Ausgang als Zufallsbitsignal ein weiteres Rückkopplungssignal in Abhängigkeit von einem anderen Ausgangsbitsignal erzeugt wird und/oder das Rückkopplungssignal an einen anderen Eingangsanschluss rückgekoppelt wird.

Beispielsweise kann die Konfiguration der Rückkopplungsdatenpfade nach einem jeweiligen Abgreifen oder Samplen des oder der Zufallsbits verändert werden. Dies kann beispielsweise durch ein Schaltnetzwerk oder andere geeignete Einrichtungen erfolgen. Denkbar sind beispielsweise Multiplexer oder steuerbare Schalter, die ein Rückkopplungsnetzwerk von Ausgangsanschlüssen des Multiplizierers zu Eingangsanschlüssen realisieren.

Es ist ferner eine Vorrichtung zum Erzeugen eines Zufallsbits vorgeschlagen, welche umfasst:

Eine kombinatorische Multiplikationseinrichtung zum Multiplizieren von zwei Eingangsworten zu einem Ausgangswort, welche zumindest zwei Eingänge und einen Ausgang umfasst;

eine Rückkopplungseinrichtung, welche derart eingerichtet ist, dass in Abhängigkeit von mindestens einem an den Ausgang abgreifbaren Ausgangsbitsignal ein Rückkopplungssignal erzeugt wird und an einen Eingang der kombinatorischen Multiplikationseinrichtung angekoppelt wird. Dabei ist ein Ausgangsbitsignal an dem Ausgang als Zufallsbitsignal abgreifbar.

Die Vorrichtung ist insbesondere eingerichtet, ein Verfahren nach einem der vorhergehenden Aspekte des Verfahrens zum Erzeugen von Zufallsbits durchzuführen.

Es ist möglich, ferner eine Steuereinrichtung, wie einen Mikroprozessor oder Controller vorzusehen, der die Rückkopplung und das Abtasten bzw. andere der vorgenannten Verfahrensaspekte realisiert oder koordiniert.

Durch die Verwendung und Beschaltung eines kombinatorischen Multiplizierers lassen sich leicht und zuverlässig echte Zufallszahlen generieren. Insbesondere ist der Schaltungsaufwand gegenüber dediziert vorgesehenen Zufallszahlengeneratoren reduziert. Dadurch eignet sich die Durchführung des vorgeschlagenen Verfahrens bzw. Implementierung der Vorrichtung zum Erzeugen von Zufallsbits insbesondere in FPGA-Einrichtungen, welche beispielsweise festverdrahtete Multiplizierer umfassen.

Die Vorrichtung kann in Ausführungsformen ferner eine oder mehrere Abtasteinrichtungen zum Abtasten von dem mindestens einen Ausgangsbitsignal umfassen. Es ist ferner denkbar, dass Invertereinrichtungen in einem Signalpfad zwischen einem Ausgang und einem Eingang gekoppelt sind. Bevorzugt ist die Vorrichtung zum Erzeugen von Zufallsbits Teil einer FPGA-Einrichtung, und die kombinatorische Multiplikationseinrichtung ist als festverdrahtete Schaltung implementiert.

Als kombinatorische Multiplizierer kommen übliche nicht getaktete Logikschaltkreise in Frage. Vorzugsweise sind dies nicht konfigurierbare Logikgatter, um eine besonders kurze Signallaufzeit für die Multiplikationsoperation zu erzielen. Insbesondere können in entsprechenden Schaltungsanordnungen die kombinatorischen Multiplikationseinrichtungen einerseits zur Zufallszahlenerzeugung verwendet werden und andererseits konventionell als Multiplizierer zum Erzeugen von Multiplikationsergebnissen aus zwei Eingangsgrößen. Insgesamt erreicht man eine zuverlässige Erzeugung von Zufallsbits, die mit einer hohen Datenrate erzeugt werden können und aufwandsgünstig implementierbar ist.

Weitere mögliche Implementierungen der Erfindung umfassen auch nicht explizit genannte Kombinationen von zuvor oder im Folgenden bezüglich der Ausführungsbeispiele beschriebenen Verfahrensschritte, Merkmale oder Ausführungsformen des Verfahrens oder des Zufallsbitgenerators. Dabei wird der Fachmann auch Einzelaspekte als Verbesserungen oder Ergänzungen zu der jeweiligen Grundform der Erfindung hinzufügen oder abändern.

Die oben beschriebenen Eigenschaften, Merkmale und Vorteile dieser Erfindung sowie die Art und Weise, wie diese erreicht werden, werden klarer und deutlicher verständlich im Zusammenhang mit der folgenden Beschreibung der Ausführungsbeispiele, die im Zusammenhang mit den Zeichnungen näher erläutert werden.

Dabei zeigen:

Fig. 1 eine schematische Darstellung eines ersten Ausführungsbeispiels für eine Vorrichtung zum Erzeugen von Zufallsbits und Darstellungen von Binärzahlen zum Erläutern eines Verfahrens zum Erzeugen von Zufallsbits;

Fig. 2 eine schematische Darstellung eines zweiten Ausführungsbeispiels für eine Vorrichtung zum Erzeugen von Zufallsbits;

Fig. 3 eine schematische Darstellung eines dritten Ausführungsbeispiels für eine Vorrichtung zum Erzeugen von Zufallsbits und Darstellungen von Binärzahlen zum Erläutern eines Verfahrens zum Erzeugen von Zufallsbits;

Fig. 4-6 zeitliche Verläufe von Zufallsbitsignalen, welche gemäß Ausführungsbeispielen des Verfahrens und der Vorrichtung zum Erzeugen von Zufallsbits erzeugt sind; und

Fig. 7 einen mittleren zeitlichen Verlauf von Zufallsbitsignalen, welche gemäß Ausführungsbeispielen des Verfahrens und der Vorrichtung zum Erzeugen von Zufallsbits erzeugt sind.

Die Figur 1 zeigt eine schematische Darstellung eines ersten Ausführungsbeispiels für eine Vorrichtung 1 zum Erzeugen von Zufallsbits und Darstellungen von Binärzahlen, welche von der Vorrichtung verarbeitet werden zum Erläuterungsverfahren zum Erzeugen von Zufallsbits.

Die Vorrichtung 1, welche auch als Zufallsbit- oder Zufallszahlengenerator bezeichnet werden kann, umfasst dabei insbesondere einen kombinatorischen Multiplizierer 2. Ein kombinatorischer Multiplizierer oder Multiplikationseinrichtung oder Multiplikationsrechenwerk erzeugt aus zwei binären Eingangsgrößen eine binäre Ausgangsgröße. Dabei wird beispielsweise ein Multiplikand A mit vorgegebener Bitbreite N mit einem Multiplikator B vorgegebener Bitbreite N multipliziert, woraus sich ein Produkt C der Bitbreite N+M ergibt. Man spricht bei Multiplikand A und Multiplikator B auch von Faktoren A, B, die ein Produkt C ergeben.

In der Darstellung der Figur 1 umfasst der kombinatorische Multiplizierer 2 einen Eingang 3 zum Empfangen von Eingangsbitsignalen AS. Obgleich dies in der Figur 1 nicht explizit dargestellt ist, sind gemäß der Bitbreite N Eingangsanschlüsse am Eingang 3 vorgesehen. Ferner ist ein zweiter Eingang 4 vorgesehen zum Empfangen des zweiten Faktors in der Art von Bitsignalen BS der Bitbreite M. An einem Ausgang 5 des Multiplizierers 2 ist das Ergebnis als Ausgangsbitsignale CS abgreifbar. Aus dem Produkt der jeweils ein Eingangswort A, B darstellenden Eingangsbitsignale AS, BS ergeben sich N+M Ausgangsbitsignale.

In der Darstellung von Figur 1 sind die zu multiplizierenden Eingangsworte A, B schematisch oberhalb der Signale AS, BS

angedeutet. Das Eingangswort A umfasst N Bits A1 bis AN, und das Eingangswort B umfasst M Bits B1 bis BM. Das Multiplikationsergebnis, also das Ausgangswort C hat somit N+M also C1 bis CN+M Bits. Die Bits werden in der Art von Signalen durch logische Pegel H oder L bzw. 1 oder 0 dargestellt.

Bei dem Verfahren zum Erzeugen von Zufallsbits ist nun vorgesehen, dass in Abhängigkeit von dem Multiplikationsergebnis die Eingangswerte erzeugt bzw. rückgekoppelt werden. In der beispielhaften Darstellung der Figur 1 ist zum Beispiel das zweitniedrigste Bit C2 bzw. das entsprechende Ausgangsbitsignal als Rückkopplungssignal RS an den Eingang 3 zurückgeführt. In der Darstellung der Binärzahlen A, B, C in Figur 1 wird somit das Ergebnisbit C2 als Eingangsbit A2 verwendet. Durch die Rückkopplung können nicht deterministische Schwingungen entstehen, so dass die Signale CS, welche den Ausgangsbits C1-CN+M entsprechen, einen gewissen Zufall haben. Man kann nun beispielsweise das Ausgangsbitsignal, welches dem P-ten Ausgangsbit CP entspricht, abgreifen und als Zufallsbit betrachten. Durch regelmäßiges Abgreifen des mit sich selbst zurückgekoppelten Multiplizierers 2 kann eine Zufallsbitfolge erstellt werden, die als binäre Zufallszahl verwendet werden kann. In der Figur 1 ist beispielhaft angedeutet, dass nach Q-maligem Abtasten oder Abgreifen des P-ten Ergebnisbits eine binäre Zufallszahl ZZ erzeugt wird.

Bei der Vorrichtung 1 zum Erzeugen von Zufallsbits kann beispielsweise beim Betrieb eines FPGAs der in der Regel vorhandene kombinatorische Multiplizierer 2 entsprechend verschaltet werden und als Zufallszahlengenerator verwendet werden. Nachdem eine Zufallszahl ZZ der gewünschten Breite oder Länge Q erzeugt wurde, kann der Multiplizierer 2 wieder konventionell zum Multiplizieren von zwei Eingangsgrößen zu einem Produkt verwendet werden. Insbesondere bei FPGAs ist so keine zusätzliche Einrichtung zum Erzeugen von Zufallszahlen notwendig. Vielmehr ergibt sich durch die Zweckentfremdung der in der Regel vorhandenen Multiplizierschaltung 2 eine einfache und zuverlässige Möglichkeit, Zufallsbits zu erzeugen.

Vorzugsweise erfolgt die Rückkopplung derart, dass keine Fixpunkte bei der Oszillation auftreten. Gegenüber konventionellen Verfahren oder Vorrichtungen zum Erzeugen von Zufallszahlen beispielsweise durch Ringoszillationen mit Hilfe von Ringoszillatoren, Fibonacci- oder Galoise-Oszillatoren ist keine zusätzliche Hardware notwendig. Vielmehr kann ein konventioneller Multiplizierer, der kombinatorisch aufgebaut ist, verwendet werden. Auf die Implementierung einer entsprechenden Multiplziereinrichtung wird nicht weiter eingegangen. Es lassen sich dabei bekannte kombinatorische Multiplizierer aufwandsgünstig einsetzen. Die im jeweiligen Multiplizierer 2 vorgesehenen Gatter sind dabei vorzugsweise festverdrahtet und nicht rekonfigurierbar wie Logikgatter in FPGAs. Dadurch wird eine erhöhte Erzeugungsrate von Zufallsbits erzielt.

Die Figur 2 zeigt eine schematische Darstellung eines zweiten Ausführungsbeispiels für einen Zufallszahlengenerator 100. In der Figur 2 sind die jeweiligen Eingangs- und Ausgangsanschlüsse einer eingesetzten Multiplziereinrichtung 2 explizit dargestellt. Der Zufallszahlengenerator 100 umfasst dabei einen kombinatorischen Multiplizierer 2 mit zwei Eingängen 3, 4 und einem Ausgang 5. Der kombinatorische Multiplizierer 2 ist eingerichtet, um zwei fünf Bit breite Eingangsworte A, B miteinander zu multiplizieren.

Die Eingangsworte A, B sind in der Figur 2 links schematisch mit ihren Bits A1-A5 und B1-B5 angedeutet. Elektrisch oder elektronisch werden die logischen Zustände der Bits mit Hilfe von Bitsignalen AS1-AS5, BS1-BS5 dargestellt. Ein vorgegebener Pegel entspricht dabei beispielsweise einer 1 oder einem H-Zustand und ein zweiter vorgegebener Pegel einem 0- oder L-Zustand. Man spricht auch von Eingangsworten der Bitbreite 5. Der kombinatorische Multiplizierer 2 liefert an seinem Ausgang 5 ein zehn Bit breites Ergebnis. Das Ergebniswort C ist in der Figur 2 schematisch als Bits C1-C10 angedeutet. Der

Ausgang 5 hat dabei zehn Anschlüsse, an denen jeweils ein Ausgangsbitsignal CS1-CS10 abgreifbar ist.

Zum Erzeugen von Zufallsbits werden nun eines oder mehrere der Ausgangsbits bzw. Ausgangbitsignale CS1-CS10 auf Eingangsanschlüsse direkt oder mittelbar rückgekoppelt. Es ist vorteilhaft, wenn durch die Rückkopplung und die entstehende Schwingung des kombinatorischen Netzwerkes des Multiplizierers 2 kein Fixpunkt auftritt. Ein offensichtlicher Fixpunkt entsteht wenn alle Eingangsbits eines Eingangswortes beispielsweise B1...B5 = 0 sind. Dann ergibt sich in der Darstellung der Figur 2 ein Produkt mit C1...C10 = 0 und durch die Rückkopplungssignale RS2, RS5, RS7, RS8, RS9, RS10 ebenfalls A1...A5 = 0. Dieser Fixpunkt kann, wie in der Figur 2 dargestellt ist, eliminiert werden, indem zwei Rückkopplungsleitungen invertiert werden. Insofern ist ein erster Inverter 19 im Rückkopplungspfad zwischen dem Ausgangsbitsignal CS1, welches dem niedrigstwertigsten Ergebnisbit C1 entspricht und dem Eingangsbitsignal BS1, welches dem niedrigwertigsten Bit B1 entspricht, vorgesehen. Analog ist ein Inverter 18 im Rückkopplungspfad von dem zweitniedrigsten Bit C2 bzw. dem entsprechenden Ausgangsbitsignal CS2 zu dem zweitniedrigstwertigen Bit A2 bzw. dem Eingangsbitsignal AS2 vorgesehen. Durch diese Maßnahme wird ein Fixpunkt verhindert.

Darüber hinaus sind auch die übrigen Ausgangsbitsignale CS3-CS10, wie in der Figur 2 dargestellt ist, an Eingangsanschlüsse der Eingänge 3, 4 zurückgekoppelt. Dadurch ergibt sich eine nicht-fixpunktbehaftete Oszillation, die nicht deterministisch ist. Das heißt man kann beispielsweise eines oder mehrere Ausgangsbitsignale CS1-CS10 abtasten und als Zufallsbitsignal ZBS verwenden. Um beispielsweise die Laufzeit und damit die Erzeugungsrate von Zufallbits zu verbessern, werden beispielsweise niedrigwertige Ergebnisbits auf niedrigwertige Eingangsbits abgebildet. In der Verschaltung erfolgt somit eine Rückkopplung von Ausgangsanschlüssen des Multiplizierers 2, die niedrigen Bitwerten entsprechend auf

Eingangsanschlüsse der Eingänge 34, welche ebenfalls niedrigen Bitwerten entsprechen. In Ausführungsformen wird zur Verbesserung der Zufälligkeit zusätzlich mindestens eine Rückkopplung von niedrigsignifikanten Bits des Ergebniswortes auf hochsignifikante Bits der Eingangsworte vorgenommen.

Die Zufallsbits können beispielsweise mit konstantem Takt des dauernd schwingenden rückgekoppelten Multiplizierers 2 abgegriffen werden. Es ist alternativ oder zusätzlich möglich, das Abgreifen der Zufallsbits nach Ablauf eines vorgegebenen Zeitintervalls vorzunehmen, nach der der Multiplizierer 2 aus einem festen Grundzustand neu gestartet bzw. zur Schwingung angeregt wird. Ein möglicher Startzustand ist beispielsweise ein Eingangswort, das nur Null oder L-Bits umfasst.

In der Figur 3 ist eine weitere Ausführungsform eines Zufallsbitgenerators 101 schematisch dargestellt. Wie bereits bei der Figur 1 ist auf die explizite Darstellung der Eingangsanschlüsse verzichtet worden. Der Zufallszahlen- oder Zufallsbitgenerator 101 umfasst insbesondere einen kombinatorischen Multiplizierer 2 mit Eingängen 3, 4 und einem Ausgang 5. Die Eingänge 3, 4 haben jeweils eine Anzahl von Eingangsanschlüssen, die der Bitbreite des jeweiligen Eingangswortes entspricht und der Ausgang 5 Ausgangsanschlüsse, die der Bitbreite des Multiplikationsergebnisses entspricht.

Beim Betrieb des Multiplizierers 2 als Zufallszahlengenerator werden eines oder mehrere der Ausgangsbitsignale auf Eingangsbitsignale rückgekoppelt. Dazu ist eine Rückkopplungsschaltung 20 vorgesehen. Die Rückkopplungsschaltung 20 umfasst dabei eine Steuereinrichtung 6, beispielsweise einen Mikrocontroller oder Prozessor, der mindestens eine Rückkopplungsleitung RS zu oder abschaltet. Dazu ist ein steuerbarer Schalter 7 vorgesehen, der über ein Steuersignal CT1 ansteuerbar ist. Um beispielsweise regelmäßig den Multiplizierer 2 in einen wohl definierten Zustand zu versetzen, ist ein Mehrfach-UND-Gatter 9 vorgesehen, welches Eingangsbitsignale BS mit einem Nullsignal NS verundet. Das

heißt, am Ausgang des UND-Gatters 9 liegen alle Bitpositionen auf Null. Ist der vorgesehene steuerbare Schalter 8, welcher von der Steuereinrichtung 6 über ein Steuersignal CT2 angekoppelt wird, mit dem UND-Gatter 9 verbunden, liegen alle Eingangsbits B1-BM des Eingangswortes B auf 0. Insofern ergibt sich auch am Ausgang 5 ein Ergebniswort C mit C1...CM+N = 0.

Wird nun die Oszillation gestartet, das heißt eines oder mehrere Ergebnisbits CP, CQ werden auf Eingangsbits des anderen Eingangswortes A abgebildet, ergibt sich eine nicht deterministische Oszillation. Das heißt, prinzipiell sind die Pegel der Ausgangsbitsignale des Ausgangssignals CS nicht vorhersehbar. Eine Abtast- oder Sample-Einrichtung 10 ist vorgesehen, um beispielsweise periodisch und/oder von der Steuereinrichtung über ein geeignetes Steuersignal CT3 gesteuert, die Pegel der Ausgangsbitsignale CS zu erfassen. Dazu hat die Abtasteinrichtung 10 einen ersten Eingang 11 zum Einkoppeln des bzw. der Ausgangsbitsignale CS und einen Steuereingang 13.

Am Ausgang werden Q Zufallsbitsignale erfasst und einer Bewerteeinrichtung 17 zugeführt. Die Bewerteeinrichtung 17 entscheidet jeweils ob der Pegel, welcher durch die Abtasteinrichtung 10 gesampled bzw. abgetastet wurde, einer logischen Null oder einer logischen Eins entspricht. Schließlich kann eine Zufallszahl der Bitbreite Q von der Bewertungseinrichtung 17 abgegriffen werden.

In den folgenden Figuren 4-6 sind Spannungsverläufe von einer in dem Ausgangsanschluss eines rückgekoppelten Multiplikationsrechenwerks abgegriffenen Bitsignalen dargestellt. Die Figur 7 zeigt einen gemittelten Spannungsverlauf über zehntausend Neustarts der erzeugten nicht-deterministischen Schwingung durch ein rückgekoppeltes Multiplikationsrechenwerk.

Zur Erzeugung der Figuren 4-7 wurden kombinatorische Multiplizierer mit zwei 18-Bit Eingangsworten und einem 36-Bit Ausgangswort betrachtet. Bits der Ausgangsworte wurden

teilweise invertiert und auf Eingangsbits abgebildet. Ein Ruhe- oder Startzustand wird durch Verunden aller 18 Bits eines Eingangs (vgl. UND-Gatter 9 in Figur 3) eingestellt. Dadurch werden alle Bits eines Eingangs auf den logischen Wert Null gezwungen, so dass sich auch das Ergebnis mit dem Wert Null einstellt. Nach Entkoppeln des UND-Gatters (vgl. UND-Gatter 9 und steuerbarer Schalter 8 der Figur 3) ergibt sich eine nicht periodische komplexe Schwingung der Output-Bits, welche über ein jeweiliges Ausgangsbitsignal elektrisch wiedergegeben sind. Die Figuren 4-7 zeigen eines der Output-Bits bzw. den jeweiligen Pegel des Ausgangsbitsignals. Dieses Ausgangsbitsignal wird als Zufallsbitsignal ZBS betrachtet.

Das Zufallsbitsignal ZBS schwankt zwischen dem in den Figuren mit beliebigen Einheiten angenommenen Pegeln, welche jeweils einer logischen Null oder Eins entsprechen. Es sind jeweils Zeitabschnitte von 100 ns nach dem Anstoßen der Rückkopplung und Schwingung bei t=0 dargestellt. Man erkennt beispielsweise in der Figur 4, dass ein nicht nachvollziehbarer Spannungsverlauf ZBS ab t=0 über das Zeitfenster von 90 ns erfolgt.

Es ergibt sich ein weiterer unterschiedlicher Spannungsverlauf, wie er in der Figur 5 dargestellt ist, nach einem weiteren Neustart des rückgekoppelten Multiplizierers, wie in der Figur 5 dargestellt ist. In der Figur 6 ist noch ein weiterer Neustart bzw. der Pegelverlauf eines der Zufallsbits ZBS angedeutet. Man erkennt anhand der Figuren 4-6, dass insbesondere nach einer Anfangszeitspanne von etwa 50 ns die Signale einen völlig unterschiedlichen Verlauf nehmen.

Vorzugsweise wird somit beim Erzeugen der Zufallsbits, also einem Abgreifen der Pegel des Zufallsbitsignals ZBS ein vorgegebener Zeitraum nach dem Start, also Rückkoppeln des Multiplizierers abgewartet. Beispielsweise kann ein Zeitraum von 100 ns zwischen Start und Abgreifen des Zufallsbitsignalpegels sinnvoll sein. Andere Werte sind jedoch ebenso denkbar.

In der Figur 7, die ein Mittelwert des Zufallsbitsignals ZBS, welches einen Mittelwert über 10000 Neustarts zeigt, erkennt man, dass insbesondere ab etwa 50-60 ns völlige Zufälligkeit besteht. Es ergibt sich praktisch ein Mittelwert der Pegel, welcher konstant verläuft. Insofern ergibt sich insbesondere nach einer vorgegebenen Zeitspanne und Einstellen einer Rückkopplungsschwingung des kombinatorischen Multiplizierers ein nicht deterministischer zufälliger Verlauf Ausgangsbitpegel. Durch regelmäßiges Abtasten können Zufallsbits mit hoher Datenrate erzeugt werden.

Insgesamt ergibt sich durch die Verwendung von einem kombinatorischen Multiplizierer, welcher zumindest teilweise rückgekoppelt wird, eine einfache aufwandsgünstige Möglichkeit, Zufallsbits zu erzeugen. Man erhält echte Zufallszahlen ohne ddizierte Schaltungen wie sie beispielsweise bei rückgekoppelten Ringoszillatoren oder Abwandlungen notwendig sind. Durch das (wiederholte) Neustarten der rückgekoppelten Multiplizierer aus einem wohl definierten Anfangszustand und Abwarten über einen vorgegebenen Zeitraum bis zum Abtasten des jeweiligen Zufallsbits ergibt sich eine gute Zuverlässigkeit und Zufälligkeit der Daten. Der vorgegebene Zeitraum kann beispielsweise experimentell ermittelt werden kann. Das Verfahren kann insbesondere aufwandsgünstig in FPGAs implementiert werden, die festverdrahtete kombinatorische Multiplziereinrichtungen umfassen.

Obwohl die Erfindung im Detail durch das bevorzugte Ausführungsbeispiel näher illustriert und beschrieben wurde, so ist die Erfindung nicht durch die offenbarten Beispiele eingeschränkt und andere Variationen können vom Fachmann hieraus abgeleitet werden, ohne den Schutzumfang der Erfindung zu verlassen.

Patentansprüche

1. Verfahren zum Erzeugen eines Zufallsbits umfassend:

Bereitstellen einer kombinatorischen Multiplikationseinrichtung (2) zum Multiplizieren von zwei Eingangsworten (A, B) zu einem Ausgangswort (C) mit zumindest zwei Eingängen (3, 4) und einem Ausgang (5);

Erzeugen von mindestens einem Rückkopplungssignal (RS1) in Abhängigkeit von mindestens einem Ausgangsbitsignal (CS1), welches an dem Ausgang (5) abgreifbar ist;

Rückkoppeln des Rückkopplungssignals (RS1) an einen Eingang (4) der kombinatorischen Multiplikationseinrichtung (2); und

Abgreifen von mindestens einem Ausgangsbitsignal (CS1) an dem Ausgang (5) als Zufallsbitsignal (ZBS).

2. Verfahren nach Anspruch 1, wobei mehrere Rückkopplungssignale (RS1, RS2) in Abhängigkeit von verschiedenen Ausgangsbitsignalen (CS1, CS2) erzeugt und rückgekoppelt werden.

3. Verfahren nach Anspruch 1 oder 2, wobei das Erzeugen des Rückkopplungssignals (RS1) umfasst: Invertieren des mindestens einen Ausgangsbitsignals (CS1).

4. Verfahren nach einem der Ansprüche 1 - 3, wobei das Abgreifen zum Erzeugen einer Zufallsbitfolge mehrfach erfolgt.

5. Verfahren nach einem der Ansprüche 1 - 4, ferner umfassend: UND-Verknüpfen von Eingangsbitsignalen (BS) und/oder des Rückkopplungssignals (RS) mit einem Referenzsignal (NS) an mindestens einem Eingang.

6. Verfahren nach Anspruch 5, wobei das Abgreifen und das UND-Verknüpfen gleichzeitig erfolgen.

7. Verfahren nach einem der Ansprüche 1 - 6, wobei eines oder mehrere Rückkopplungssignale (RS) derart erzeugt und rückge-

koppelt werden, dass das Zufallsbitsignal (ZBS) keinen Fixpunkt erreicht.

8. Verfahren nach einem der Ansprüche 1 - 7, wobei die Eingänge (3, 4) eine vorgegebene Bitbreite zum Empfangen von Eingangsbitsignalen (AS1-AS5, BS1-BS5) aufweist und der Ausgang (5) eine vorgegebene Bitbreite zum Ausgeben von Ausgangsbitsignalen (C1-C10) aufweist, und das Verfahren ferner umfasst:

Erzeugen eines ersten Rückkopplungsbitsignals (RS1) in Abhängigkeit von einem Ausgangsbitsignal (CS1), welches einem niedrigstwertigen Bit (C1) des Ausgangsworts (C) entspricht, und Rückkoppeln des ersten Rückkopplungsbitsignals (RS1) an einen Eingangsanschluss, welcher einem niedrigstwertigen Bit (B1) eines Eingangsworts (B) entspricht; und

Erzeugen eines zweiten Rückkopplungsbitsignals (RS2) in Abhängigkeit von einem Ausgangsbitsignal (CS2), welches einem zweitniedrigstwertigen Bit (C2) des Ausgangsworts (C) entspricht, und Rückkoppeln des zweiten Rückkopplungsbitsignals (RS2) an einen Eingangsanschluss, welcher einem zweitniedrigstwertigen Bit (A2) des anderen Eingangsworts (A) entspricht.

9. Verfahren nach einem der Ansprüche 1 - 8, ferner umfassend: Abgreifen von mehreren Ausgangsbitsignalen (CS1-CS10), welche unterschiedlichen Bits (C1-C10) des Ausgangsworts (C) entsprechen, an dem Ausgang (5) als mehrere Zufallsbitsignale.

10. Verfahren nach einem der Ansprüche 1 - 9, wobei nach dem Abgreifen von dem mindestens einen Ausgangsbitsignal (CS1) an dem Ausgang (5) als Zufallsbitsignal ein weiteres Rückkopplungssignal in Abhängigkeit von einem anderen Ausgangsbitsignal erzeugt wird und/oder das Rückkopplungssignal an einen anderen Eingangsanschluss rückgekoppelt wird.

11. Vorrichtung (1, 100, 101) zum Erzeugen eines Zufallsbits mit:

einer kombinatorischen Multiplikationseinrichtung (2) zum Multiplizieren von zwei Eingangsworten (A, B) zu einem Ausgangswort (C), welche zumindest zwei Eingänge (3, 4) und einen Ausgang (5) umfasst;

einer Rückkopplungseinrichtung (20), welche eingerichtet ist, in Abhängigkeit von mindestens einem an dem Ausgang (5) abgreifbaren Ausgangsbitsignal (CS1), ein Rückkopplungssignal (RS1) zu erzeugen und an einen Eingang (3) der kombinatorischen Multiplikationseinrichtung (2) einzukoppeln;

wobei ein Ausgangsbitsignal (AS1) an dem Ausgang als Zufallsbitsignal (ZBS) abgreifbar ist.

12. Vorrichtung (1, 100, 101) nach Anspruch 11, welche eingerichtet ist, ein Verfahren nach einem der Ansprüche 1 - 10 durchzuführen.

13. Vorrichtung (1, 100, 101) nach Anspruch 11 oder 12, ferner mit einer Abtasteinrichtung (10) zum Abtasten von mindestens einem Ausgangsbitsignal.

14. Vorrichtung nach einem der Ansprüche 1 - 13, ferner mit mindestens einer Invertereinrichtung (18, 19), welche in einem Signalpfad zwischen dem Ausgang (5) und einem der Eingänge (3, 4) gekoppelt ist.

15. Vorrichtung (1, 100, 101) nach einem der Ansprüche 1 - 14, wobei die Vorrichtung (1, 100, 101) Teil einer FPGA-Einrichtung ist und die kombinatorische Multiplikationseinrichtung (2) als festverdrahtete Schaltung implementiert ist.

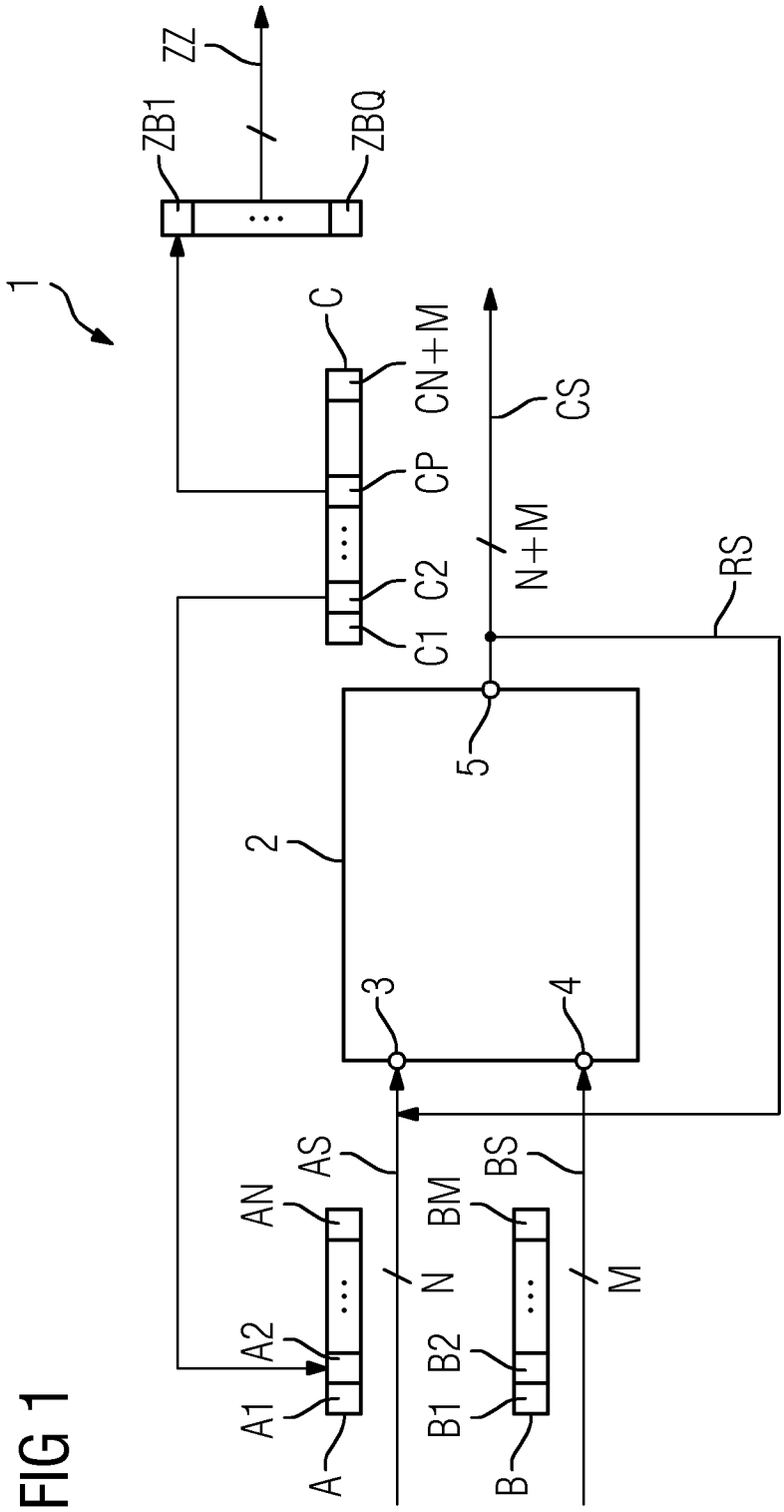


FIG 1

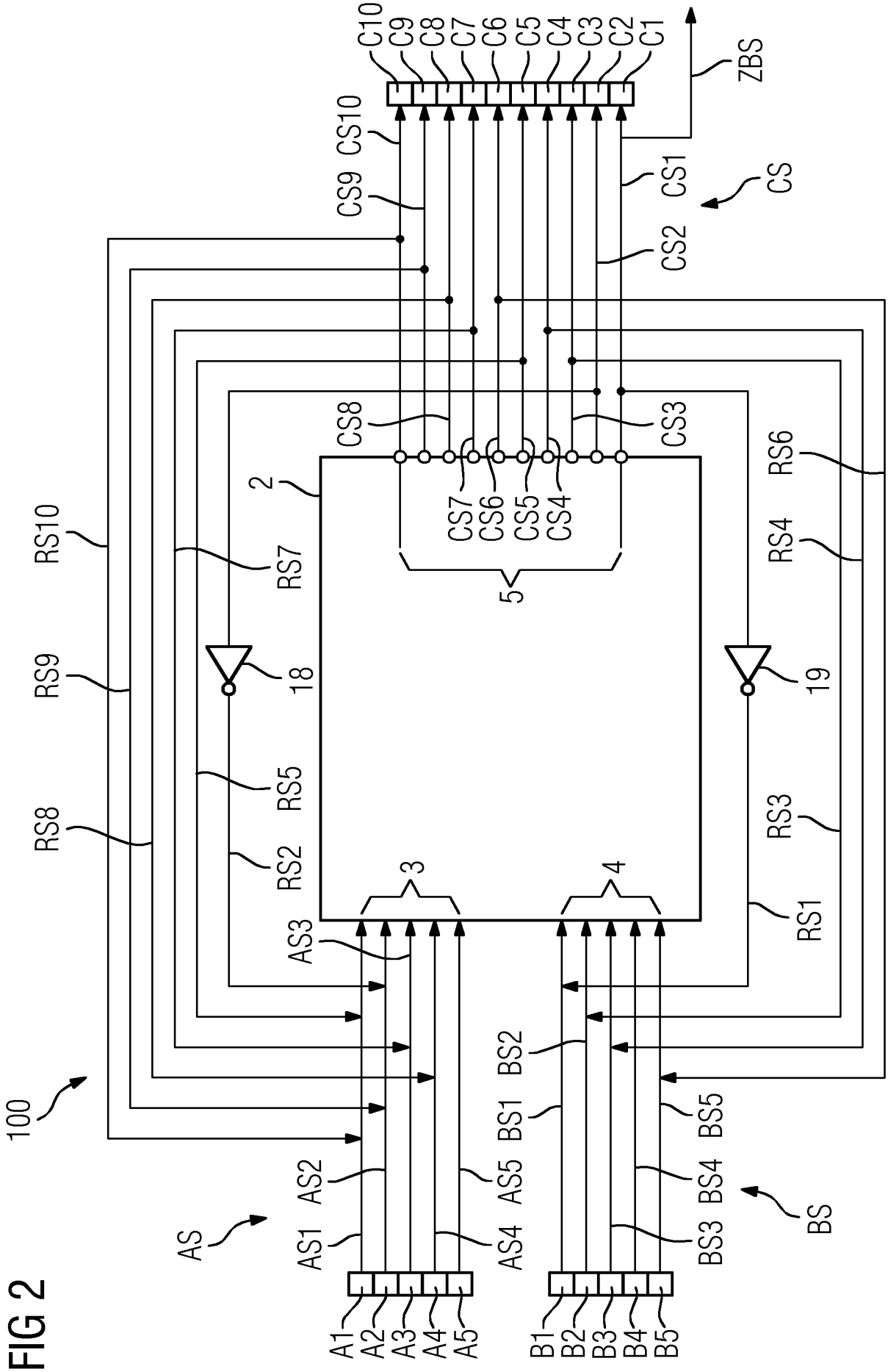

100
AS
AS1
AS2
AS3
AS4
AS5
A1
A2
A3
A4
A5
BS
BS1
BS2
BS3
BS4
BS5
B1
B2
B3
B4
B5
CS
CS1
CS2
CS3
CS4
CS5
CS6
CS7
CS8
CS9
CS10
C1
C2
C3
C4
C5
C6
C7
C8
C9
C10
ZBS
RS1
RS2
RS3
RS4
RS5
RS6
RS7
RS8
RS9
RS10
2
3
4
5
18
19

FIG 2

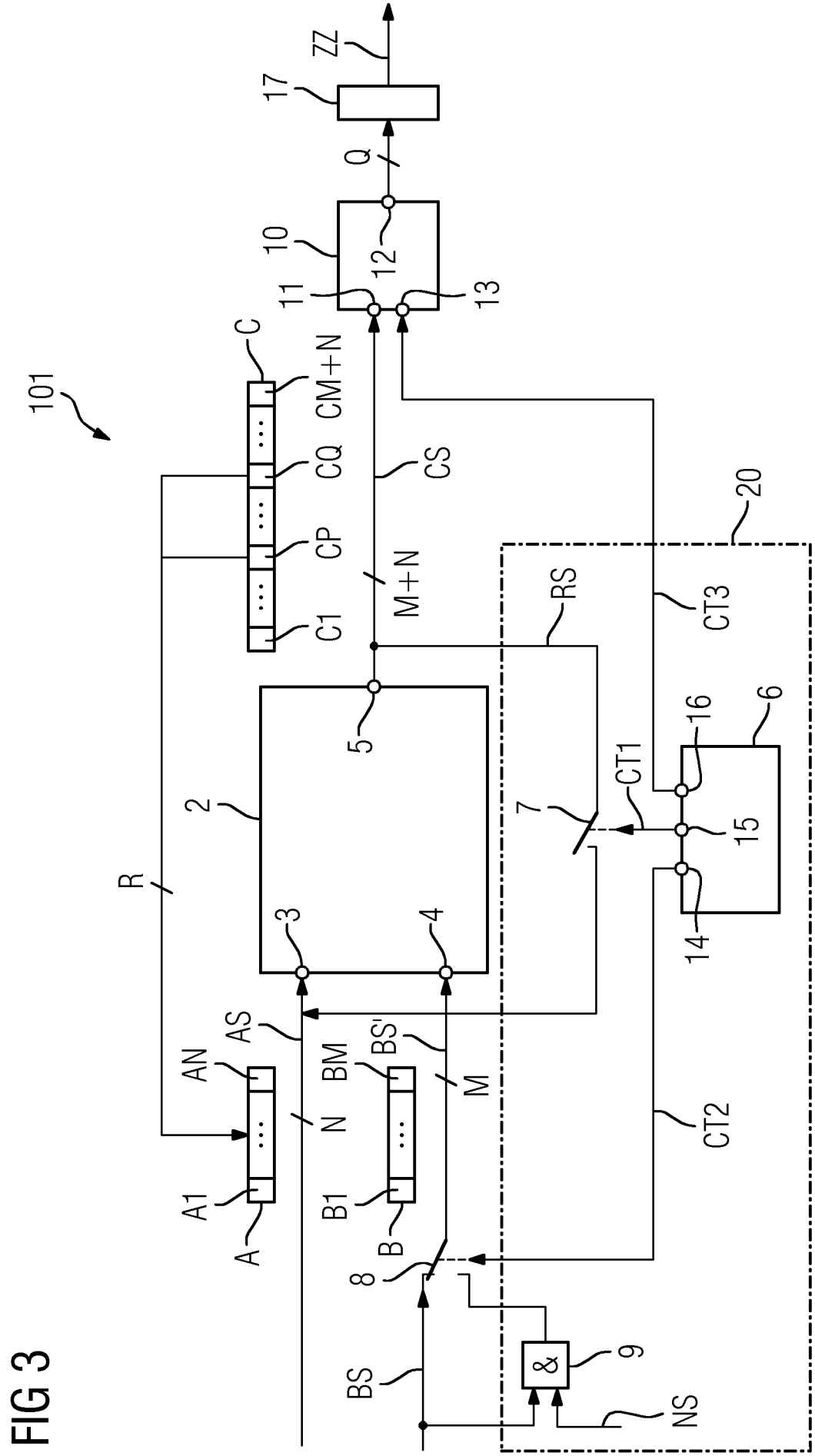

101
ZZ
17
Q
10
12
11
13
C
CM+N
CQ
CS
CP
C1
M+N
5
2
R
3
4
AS
AN
BM
BS'
N
M
A1
A
B1
B
8
BS
&
9
NS
RS
CT3
20
CT1
16
6
7
15
14
CT2

FIG 3

FIG 4

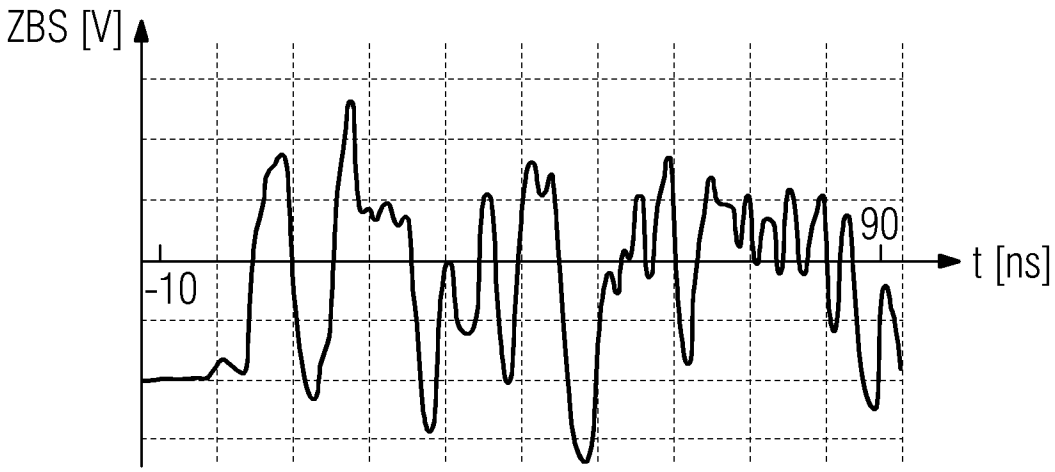


FIG 5

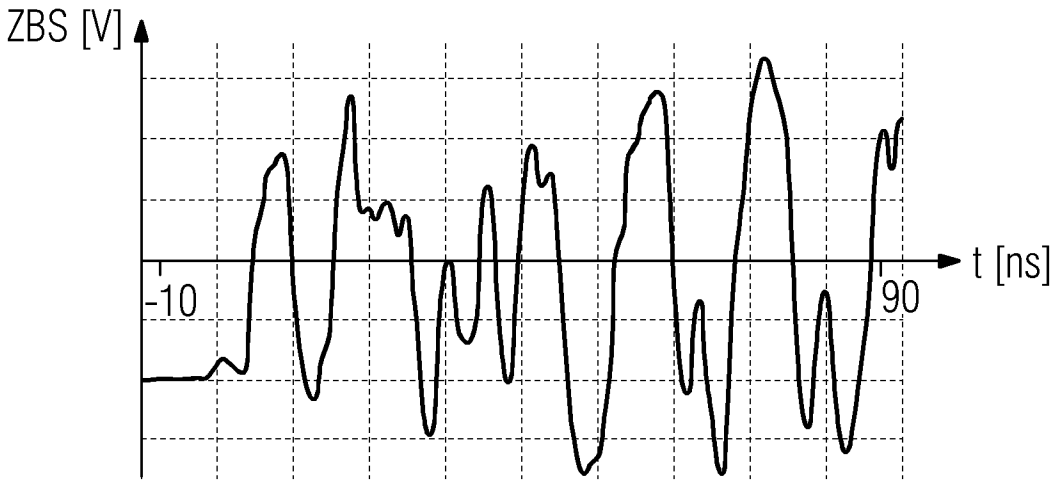


FIG 6

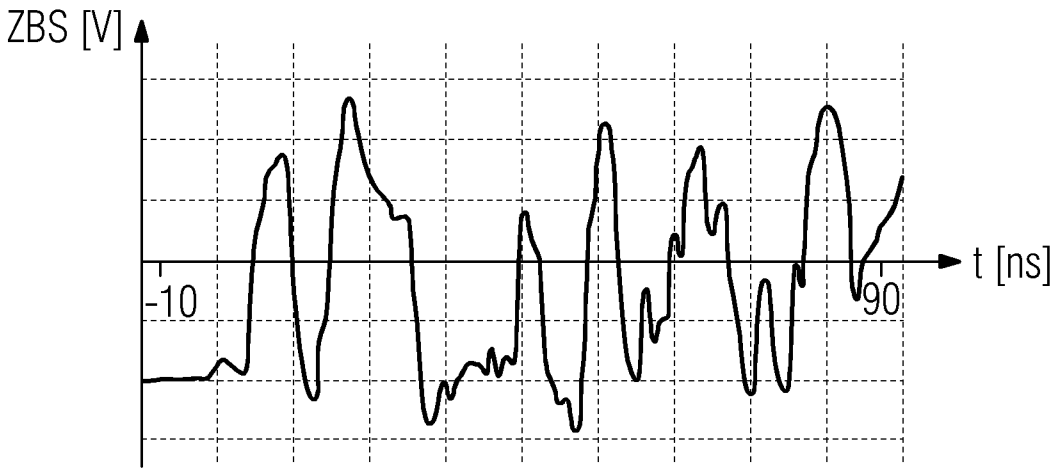
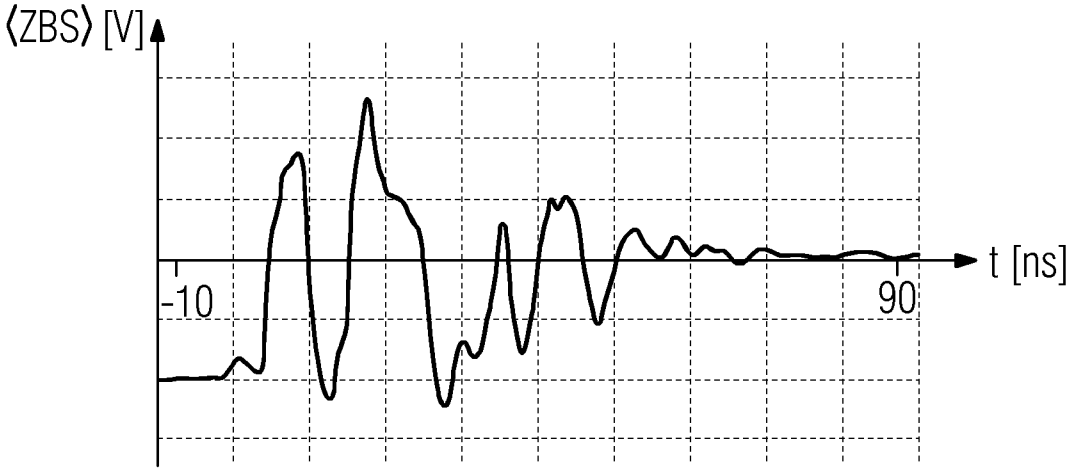


FIG 7



INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/067600

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F7/58 H03K3/84
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F H03K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 8 099 449 B1 (SCHULTZ DAVID P [US]) 17 January 2012 (2012-01-17) abstract column 2, line 43 - column 3, line 61 column 8, line 5 - line 12 figures 1,3 -----	1-15

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 October 2013	07/11/2013

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Post, Katharina

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2013/067600

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 8099449 B1	17-01-2012	NONE	

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2013/067600

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G06F7/58 H03K3/84
ADD.

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
G06F H03K

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, INSPEC

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 8 099 449 B1 (SCHULTZ DAVID P [US]) 17. Januar 2012 (2012-01-17) Zusammenfassung Spalte 2, Zeile 43 - Spalte 3, Zeile 61 Spalte 8, Zeile 5 - Zeile 12 Abbildungen 1,3 -----	1-15

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen ☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
24. Oktober 2013	07/11/2013

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Post, Katharina

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2013/067600

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 8099449 B1	17-01-2012	KEINE	