ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19)

المملكة المغربية
المكتب المغربي للملكية الصناعية و التجارية

(12) BREVET D'INVENTION

(11) N° de publication :
MA 59288 B1

(43) Date de publication :
31.08.2023

(51) Cl. internationale :
G06F 7/58; H03K 3/84; H03K 19/21

(21) N° Dépôt :
59288

(22) Date de Dépôt :
18.01.2021

(30) Données de Priorité :
17.07.2020 RU 2020123866

(86) Données relatives à la demande internationale selon le PCT:
PCT/RU2021/050010 18.01.2021

(71) Demandeur(s) :
PHYSTECH TECHNOLOGIES TRUE RANDOM AG, Bosch 71, Hunenberg, ZG 6331 (CH)

(72) Inventeur(s) :
GONCHAROV, Sergey Vladimirovich

(74) Mandataire :
H&H IP LAW

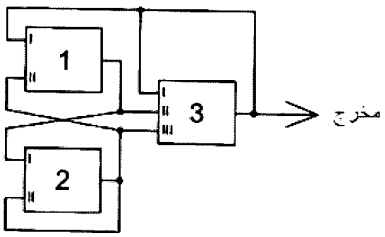
(54) Titre : **GÉNÉRATEUR DE NOMBRES VÉRITABLEMENT ALÉATOIRES**

(57) Abrégé : La présente invention concerne des dispositifs pour générer des nombres véritablement aléatoires qui comprennent une matrice booléenne autonome numérique oscillant de manière chaotique en qualité de source d'entropie. Selon l'invention, la matrice booléenne autonome numérique oscillant de manière chaotique comprend trois éléments logiques connectés les uns aux autres, dont deux sont des éléments logiques à deux entrées "et exclusif" et/ou "ou-non exclusif", tandis que le troisième élément logique possède trois entrées et une sortie et effectue une fonction logique spéciale "calcul d'unités" pendant laquelle un un logique est affiché à sa sortie si un un logique est présent sur au plus une de ses entrées, tandis qu'un zéro logique s'affiche dans le cas contraire. Le résultat technique consiste en une augmentation de la vitesse de génération de nombres véritablement aléatoires tout en diminuant la consommation énergétique.

مولد رقم عشوائي حقيقي

الملخص

يتعلق الاختراع الحالي بأجهزة لتوليد أرقام عشوائية حقيقية، وتشتمل على شبكة منطقية ذاتية التحكم رقمية متذبذبة على نحو عشوائي كمصدر للإنتروبيا. وفقًا للاختراع، تتكون الشبكة المنطقية ذاتية التحكم الرقمية المتذبذبة على نحو عشوائي من ثلاثة عناصر منطقية مرتبطة ببعضها البعض، اثنان منها يمثلان بوابتي "Exclusive OR" و/أو "Exclusive OR-NOR" ثنائيتي المخرجات، ويشتمل العنصر المنطقي الثالث على ثلاثة مدخلات ومخرج واحد، وينفذ دالة "آحاد العد" منطقية، حيث يتم ضبط مخرجها على واحد منطقي إذا كان واحد منطقي موجودًا فيما لا يزيد عن أحد مدخلاته، وإلا فسيتم تعيينه على صفر منطقي. وتتمثل النتيجة الفنية المحققة في زيادة معدل توليد الرقم العشوائي الحقيقي مع تقليل استهلاك الطاقة.



الشكل 1

مولد رقم عشوائي حقيقي

المجال التقني للاختراع

يتعلق هذا الاختراع بأجهزة لتوليد الأرقام العشوائية الحقيقية، حيث تتضمن شبكة منطقية ذاتية التحكم رقمية متذبذبة على نحو عشوائي كمصدر للإنتروبيا.

يتم استخدام الاختصارات التالية في هذا الوصف:

RNG - مولد رقم عشوائي

PRNG - مولد رقم شبه عشوائي

PLIC - دائرة متكاملة منطقية قابلة للبرمجة

ABN - شبكة منطقية ذاتية التحكم

SCO - مذبذب عشوائية متزامنة

VLSIC - دائرة متكاملة واسعة النطاق جدًا

ASIC - دائرة متكاملة خاصة بتطبيق معين

الخلفية التقنية للاختراع

هناك مولّدات رقمية للأرقام شبه العشوائية (PRNG)، معروفة من خلال المجال السابق، والتي تستند إلى بعض الدوال الدورية وتتضمن، على سبيل المثال، مولّدِ تطابق خطي، ومولّدِ سجل إزاحة تغذية مرتدة خطية، ومولّدِ سجل إزاحة تغذية مرتدة عمومية، مفتول ميرسن. يتم الحصول على أفضل النتائج باستخدام عداد أرقام بسيط مرتبط على التوالي بخوارزمية تشفير، مثل تشفير الكتلة أو دالة تجزئة أحادية الاتجاه.

والعيب الشائع لجميع مولّدات PRNGs هو حتمية التسلسل الناتج، والذي يستبعد أو يعقد بشكل كبير استخدام الأرقام شبه العشوائية لأغراض التشفير، حيث يمكن التنبؤ بالسلسلة الكاملة للأرقام شبه العشوائية إذا كانت خوارزمية الجهاز والحالة الأولية أو أي حالة سابقة لهذا المولّدِ معروفة. علاوة على ذلك، كل هذه الطرق مكلفة حسابيًا، وكلما زادت المتطلبات المفروضة على جودة الأرقام العشوائية، توجب إجراء المزيد من العمليات الحسابية.

هناك مولّدات أرقام عشوائية حقيقية معروفة، والتي تستند إلى مبادئ فيزيائية محددة. تم استخدام ظواهر فيزيائية عشوائية من الناحية التاريخية، مثل رمي النرد، والانحلال الإشعاعي،

ورقمنة الميكروفون للضوضاء السمعية المحيطة، والضوضاء الجوية التي تلتقطه الموجات قصيرة التردد، وما إلى ذلك.

ويكمن عيب هذه الأجهزة في حاجتها إلى إعداد فيزيائي خاص، جهاز استشعار، أو عاكس طاقة، وواجهة كمبيوتر. بالإضافة إلى ذلك، يمكن أن يعتمد تشغيل هذه الأجهزة بشكل كبير على الظروف البيئية. فهي تتطلب الكثير من الطاقة، وغالبًا ما تكون سرعة توليد الأرقام العشوائية بطيئة جدًا.

هناك مولّدات معروفة تستند إلى مبادئ فيزيائية، ولكنها تستخدم المكونات الإلكترونية فقط. على سبيل المثال، يستخدم نظام ERNIE 1 وجهاز كمبيوتر Ferranti Mark 1 الضوضاء الحرارية الآتي من مقاوم. في كثير من الأحيان، يتم استخدام المولّدات التي تستخدم انهمار الشحنات لوصلة موجب-سالب ذات انحياز عكسي في الصمام الثنائي Zener [1].

عيب هذه الأجهزة هو الحاجة إلى تصنيع جزء تناظري منفصل للجهاز، والذي يستبعد أو يعقد بشكل خطير تصنيع الدوائر الرقمية المتكاملة (VLSIC) التي تشتمل على RNGs. بالإضافة إلى ذلك، لا يمكن تنفيذ هذه المولّدات في دائرة متكاملة منطقية قابلة للبرمجة (PLIC).

هناك RNGs معروفة تستخدم الفرق في تردد مولّدي ذبذبات بسبب الانحراف الحراري. على سبيل المثال، تحتوي شريحة تخزين البرامج الثابتة Intel 82802 على مولّدي ذبذبات، أحدهما سريع والآخر بطيء، يقعان في أجزاء مختلفة من البلورة، ويقيسان الفرق بين ترددهما. يمكن تنفيذ RNG المذكور بالكامل عن طريق المنطق الرقمي، حيث يتم عادةً استخدام العاكسات التي لها تغذية مرتدة وسلسلة من العناصر العازلة كخط تأخير كمولّد ذبذبات.

تتضمن عيوب هذه المولّدات الحاجة إلى وضع مولّدات الذبذبات بعيدًا عن بعضها البعض في الطوبولوجيا البلورية من أجل تقليل الارتباط الحراري بينها، والأداء المنخفض، نظرًا لأنه من الضروري تراكم الانحراف خلال بعض فترات التشغيل، وضعف القدرة على التنبؤ بجودة الأرقام العشوائية. علاوة على ذلك، يصعب تطبيق هذا المولّد عمليًا في PLIC، نظرًا لأن أدوات التطوير لا تسمح بالتحكم في الوضع الفيزيائي للعناصر. كقاعدة عامة، في حالة تحديد الموضع تلقائيًا، سيتم أيضًا وضع مولّدات الذبذبات، المرتبطة منطقيًا، على مقربة من بعضها البعض، مما يستلزم ارتباطًا ترديديًا أكثر دلالة بينها.

على مدى السنوات العديدة الماضية، تم استكشاف ما يسمى "الشبكات المنطقية ذاتية التحكم" (ABN) بشكل فعال. تمثل هذه الشبكة رسمًا بيانيًا مرتبطًا طوبولوجيًا للعناصر المنطقية، حيث لا يتم توفير أي تحكم خارجي أو إشارات ساعة. في الوقت نفسه، تُفرض متطلبات إضافية واضحة على هذه الشبكة: لا ينبغي أن يكون لأي عنصر مدخلات "معلقة" (غير مرتبطة بأي مخرجات) ولا ينبغي

ربط المخرجات ببعضها البعض. هذه المتطلبات ناتجة عن يقين حالة العناصر المنطقية للشبكة والسلامة الكهربائية لتشغيلها. ويمكن أن تظهر ABN سلوكيات مختلفة اعتمادًا على مخطط الشبكات: أن تكون في حالة مستقرة أو شبه مستقرة، أو تتأرجح بتردد معين وشكل موجة، أو تكون في حالة تسمى "الفوضى المنطقية". ويُوضح مثال على أبسط ABN وهو جهاز مكرِّر بمخرج مرتبط بالمدخل. هذه الشبكة في حالة شبه مستقرة، مما يعني أنه اعتمادًا على الحالة الأولية (صفر أو 1)، ستبقى فيها إلى ما لا نهاية. هناك مثال آخر يتمثل في عاكس أو عدة عاكسات مرتبطة ببعضها البعض في حلقة. سيكون سلوك العاكسات مستقرًا أو شبه مستقر أو متذبذبًا اعتمادًا على عددها في الحلقة. من المرجح أن يكون العاكس في حالة مستقرة (بين صفر و1)، ويرجع ذلك إلى التنفيذ الفيزيائي للعاكس كمضخِّم مع نسبة كسب عالية وتغذية مرتدة سلبية تساوي 1. للسبب نفسه، قد لا يكون هناك توليد في الشبكات الصغيرة جدًا التي تحتوي على عناصر ذات معدل انتقال منخفض لإشارة الخرج. ستتذبذب الشبكة بفترة تتناسب مع عدد العاكسات في ظل وجود عدد فردي من العاكسات. وتكون الشبكة في حالة شبه مستقرة في وجود عدد زوجي من العاكسات. وكما يمكن أن نلاحظ، فإن مولد الرقم العشوائي الذي يتم تنفيذه في الدائرة المتكاملة Intel 82802 على أساس مولّدِي ذبذبات وقياس إزاحة التردد بينهما، في الواقع، يشكّل حالة خاصة من ABN. فهو يستخدم حلقتين مع عدد فردي مختلف من العاكسات. غالبًا ما تؤدي الشبكات الأكثر تعقيدًا إلى سلوكيات عشوائية.

هناك تناظر مادي مباشر موضوعي، والذي يساعد على الفهم البصري لسلوكيات ABNs في المواقف المختلفة. فيُعتبر هذا بندول. يبدأ البندول البسيط في التأرجح بفترة استقرار بعد انحرافه وإطلاقه. هذا مثال على السلوك المتذبذب. إذا أدرنا البندول لأعلى، فإن النقطة العليا تمثل حالة شبه مستقرة؛ أي انحراف صغير من شأنه أن يتسبب في سقوط البندول إلى اليسار أو اليمين. إذا قسمنا ذراع البندول إلى جزأين مرتبطين بمفصلة، فإننا نحصل على ما يسمى بالبندول العشوائي، والذي لا يمكن التنبؤ بتطوره بدقة بمرور الوقت، نظرًا لأن أي تغير متناهي الصغر في الحالة الأولية (حتى مستوى الكَمّ) يزيد بمرور الوقت ويؤدي إلى تغييرات كبيرة اعتباطيًا في سلوك البندول. من خلال هذا القياس، فمن الممكن قياس الانحرافات العشوائية في ترددات اثنين من البندولات الناتجة عن التأثيرات الخارجية العشوائية؛ ومع ذلك، سيتطلب ذلك تحليلًا شاملًا. من ناحية أخرى، من الممكن انحراف البندول العشوائي والحصول على قيمة عشوائية في أقصر فترة زمنية ممكنة.

كما يتضح من المثال المعطى، يمكن بالفعل استخدام ABNs المتذبذبة لتوليد أرقام عشوائية. ومع ذلك، تعد ABNs، التي تظهر في البداية سلوكًا على نحوٍ عشوائي، واعدة أكثر بكثير. يتم تحديد سرعة تطور العشوائية المنطقية وخصائصها النوعية من خلال عدد من العوامل، والأهم من ذلك

كله هو أس ليابونوف Lyapunov المميز. إذا كان العامل الأسي سالبًا، فإن الانحرافات تتلاشى بمرور الوقت. إذا كان العامل الأسي أكبر من الصفر، يتم تضخيم الانحرافات العشوائية بواسطة النظام. إذا كان العامل الأسي يساوي صفرًا، فإن الانحرافات لا تخمد أو تتضخم، بل تتراكم إذا دخلت النظام من الخارج. للتوليد الفيزيائي السريع للأرقام العشوائية، يجب أن يكون العامل الأسي غير سالب. للبندول البسيط له عامل سالب لأس ليابونوف، والذي يتم التعبير عنه بحقيقة أن تردد التذبذب يستقر على الفور في غياب التأثيرات الخارجية. يعد البندول العشوائي مثالًا خاصًا لنظام ذي أس موجب، بحيث يؤدي أي تأثير صغير إلى ديناميكيات مختلفة تمامًا بعد وقت قصير. في المنطق الثنائي، لا توجد دوال منطقية من شأنها تضخيم الانحرافات الصغيرة، ولكن هناك دوال لا تسمح باختفاء التغييرات الناتجة - في حالة وجود وسيطين، فهما الدالتان XOR (Exclusive "OR") وXNOR (التكافؤ). وأي تغيير في أي إشارة دخل يؤدي إلى تغيير في إشارة الخرج. لهذا السبب، يُفضل استخدام هذه الدوال في RNGs.

تُعرف دوائر ABN بأنها تُظهر السلوك العشوائي من الحالة الراهنة للعلم. تحدث العشوائية عندما يتم تحديد تشغيل الشبكة من خلال أصغر الانحرافات في جهد الإمداد والتحولات الأمامية بسبب التقلبات الحرارية والالتقاطات وعوامل أخرى مزعزعة للاستقرار. في المرجع [3]، يتم النظر في بوابات XOR أو XNOR المنطقية ثنائية وثلاثية المدخلات، حيث يتم إعادة الخرج إلى المدخلات من خلال خطي تأخير (أو ثلاثة على التوالي). في مثل هذه الشبكات، يمكن ملاحظة السلوك العشوائي عند نسبة معينة من طول خطوط التأخير. مشكلة هذه الشبكة هي الاعتماد القوي لسلوكها ليس فقط على نسبة طول خطوط التأخير، ولكن أيضًا على تنفيذها الفيزيائي، بينما بدلًا من العشوائية، يمكن أن تكون هناك تذبذبات. علاوة على ذلك، على الرغم من البساطة التخطيطية الواضحة للجهاز، فإنه يتطلب عددًا كبيرًا من العناصر المنطقية، نظرًا لأن كل خط تأخير هو عبارة عن سلسلة من العاكسات. نتيجة لذلك، يمكن أن تتكون الدائرة ذات المظهر البسيط من عدة عشرات من العناصر. علاوة على ذلك، فإن ثلاثة من بين أربع صور متغيرة من هذا المولّدِ لها عيب أساسي، وهو فقدان التوليد بعد فترة. يكتسب عنصر XOR حالة مستقرة مع صفر عند الخرج بغض النظر عن عدد المدخلات، وعنصر XNOR بمدخلين - مع وجود واحد عند المخرج. يحتوي عنصر XOR الذي يحتوي على ثلاث مدخلات على حالة مستقرة إضافية - مع وجود واحد عند المخرج. كما هو موضح في المرجع [4]، يتم ملاحظة توليد مستقر إلى حد ما في حالة عنصر XNOR ثلاثي المدخلات وخطوط تأخير تتكون من 18 و6 و2 من العاكسات.

في عام 2009، اقترح Rui Zhang et al. [2] دائرة تتكون من ثلاثة عناصر منطقية ثنائية المدخلات، حيث تحدث فيها عشوائية منطقية - بوابتان XOR وبوابة XNOR واحدة. لتنفيذ مثل

هذه الدائرة، استخدَمَ عناصر منفصلة. هذه الدائرة لها أيضًا عيوب متأصلة، والتي سيتم مناقشتها أدناه. عند تنفيذ مثل هذه الشبكة في PLIC، قد يختفي التوليد أو قد تحدث التذبذبات بدلًا من السلوك العشوائي.

في أطروحته [4]، اقترح ديفيد روزين David Rosin دائرة أكثر تعقيدًا تبدي أيضًا سلوكًا على نحوٍ عشوائي- حلقات كبيرة من عناصر XOR ثلاثية المدخلات، حيث أن كل عنصر يتلقى إشارة من نفسه ومن الجارين الأقرب له كمدخل. في هذه الحالة، يتم التقاط الإشارة الناتجة من عدة نقاط في الحلقة ويتم دمجها أيضًا من خلال عناصر XOR. ومع ذلك، هذه الدائرة غير قابلة للتشغيل، في شكلها النقي، لأن الحلقات المكونة من عدد زوجي من العناصر لها ما يصل إلى أربع حالات مستقرة مختلفة، وستستقر حتمًا في واحدة منها، وهي الحالات التي بها جميع الأصفار، وجميع الآحاد، ومتغيران من الأصفار والآحاد بالتناوب.

للقضاء على الحالة المستقرة، يستبدل Rosin أحد عناصر XOR في المولّدِ بعنصر XNOR. تعتمد جودة العشوائية الناتجة في هذا المولّدِ على عدد العناصر المنطقية في الحلقة. يقترح Rosin استخدام 16 عنصرًا. ومع ذلك، فإن الإثارة التي تنشأ في مثل هذا النظام يجب أن تمر من خلال ثمانية عناصر منطقية قبل الوصول إلى الجانب الآخر من الحلقة، وهو وقت يمكن مقارنته بدورة ساعة معالج دقيق واحدة. لذلك، فيما يتعلق بتنفيذ الأجهزة، من المستحسن الانتظار لعدة دورات ساعة لإزالة الارتباط بين القيم المتتالية. عيب كل من مولّدات Rosin وZhang هو استحالة التأثير الخارجي المزعزع للاستقرار على الشبكة.

يُعرف مولّدِ الرقم العشوائي الحقيقي من المجال السابق، والذي يتكون من شبكة منطقية ذاتية التحكم رقمية متذبذبة على نحو عشوائي كمصدر للإنتروبيا (انظر مواصفات طلب براءة الاختراع WO2019222866 المنشورة في عام 2019). كما هو الحال مع مولّدِ Rosin، يستخدم هذا المولّدِ حلقة من ثلاثة عناصر XOR وعنصر XNOR واحد وعنصر XOR لالتقاط الإشارات من الحلقة. على عكس مولّدِ Rosin، يستخدم هذا المولّدِ عاكسًا إضافيًا لتوليد إشارة دورية عالية التردد ولزعزعة استقرار الشبكة المنطقية ذاتية التحكم.

هذا الجهاز هو الأقرب من حيث المادة التقنية والنتيجة التقنية المحققة وقد تم اختياره كنموذج أولي للاختراع المقترح.

تتضمن عيوب هذا النموذج الأولي أيضًا الوقت المفرط المطلوب لتوليد أرقام عشوائية حقيقية، ومجموعة العناصر، وزيادة استهلاك الطاقة.

الكشف عن الاختراع

بناءً على هذه الملاحظة الأصلية، يتمثل الهدف الرئيسي للاختراع المقترح في توفير مولد رقم عشوائي حقيقي حيث يشتمل على شبكة منطقية ذاتية التحكم رقمية متذبذبة على نحو عشوائي كمصدر للإنتروبيا، والذي من شأنه أن يسمح على الأقل بتقليل عيب واحد على الأقل من العيوب المذكورة أعلاه، وعلى وجه التحديد، زيادة معدل توليد الرقم العشوائي الحقيقي مع تقليل استهلاك الطاقة، وهي المهمة قيد البحث.

يتمثل الهدف من هذا الاختراع في بناء ABN يمكن التحكم فيه جزئيًا، والذي سيتميز بحجم أدنى ويضمن الوصول إلى حالة فوضى منطقية بأعلى معدل ممكن. المطلب الأكثر أهمية هو استحالة الوصول إلى حالة مستقرة أو شبه مستقرة أو متذبذبة للشبكة. علاوة على ذلك، فإن معدل زيادة الفوضى يعتمد بشكل مباشر على حجم مسارات انتشار الإشارات الدورية الموجودة في الشبكة. كلما كان حجم المسار أكبر، طالت مدة انتقال الإشارة قبل العودة إلى نقطة البداية. لذلك، يجب أن تكون الشبكة صغيرة بقدر الإمكان. يصبح هذا واضحًا من النظر إلى مذبذب يتكون من عدد فردي من العاكسات: وتتناسب فترة التذبذب بشكل مباشر مع طول الحلقة.

لإجراء مزيد من التحليل، من الأفضل وضع شبكة منطقية متزامنة عين الاعتبار. يتمثل الاختلاف الفعلي بين شبكة منطقية متزامنة وشبكة ABN في أن الإشارة عند مخرجات جميع العناصر المنطقية تتغير في وقت واحد، لذلك يمكن افتراض أن الشبكة تمر بعدد من الحالات. نظريًا، عند سرعة تشغيل متطابقة للعناصر، وأطوال متطابقة لجميع الموصلات، وظروف تشغيل متطابقة للعناصر، يصبح ABN شبكة منطقية متزامنة. علاوة على ذلك، كما هو موضح في المرجع [3]، يمكن أن يؤدي التأثير المتبادل لأجزاء الشبكة المختلفة إلى تزامنها قسريًا. لهذا تأثير مهم للغاية يجب أيضًا إزالته أو تقليله لأدنى حد. ويمكن تحليل هذه الشبكات بترتيب زيادة عدد العناصر المنطقية نظرًا لأنه يتم البحث عن أصغر شبكة ممكنة. ويمكن إجراء تحليل شامل نظرًا لأن عددًا من الدوال والشبكات المنطقية والمحتملة القائمة عليها قابلة للعد والترتيب.

يمكن أن تتكون الشبكة أحادية العنصر من جهاز مكرِّر واحد أو عاكس واحد. في الحالة الأولى، لا يوجد توليد، وفي الحالة الأخيرة، هناك تذبذبات دورية. لذلك، لا يمكن لشبكة تتكون من عنصر منطقي واحد أن تولد الفوضى.

سننظر الآن في شبكة ذات عنصرين. لا يمكن أن يشتمل كل عنصر على أكثر من مدخلين، ومن الممكن وجود أربع حالات شبكة مختلفة. هناك العديد من التركيبات المحتملة للانتقالات بين هذه الحالات، ولكن يمكن تجميعها حسب الخصائص. الفئة الأولى عندما تكون هناك حالة متردية واحدة، والتي يمكن أن توجد فيها الشبكة إلى أجل غير مسمى. من الواضح أن مثل هذه الشبكات غير قابلة للاستخدام. الفئة الثانية عندما تكون هناك دورة واحدة على الأقل تتكون من حالتين أو ثلاث حالات.

في هذه الحالة، يكون أحد العناصر في حالة مستقرة، ويتذبذب العنصر الثاني، أو يتذبذب كلا العنصرين مع نفس الفترة. هذه الشبكات غير قابلة للاستخدام أيضًا. الحالة الأخيرة الممكنة هي عندما تتطور الشبكة عبر جميع الحالات الأربع. في هذه الحالة، فإن العدد الإجمالي للدورات المختلفة يساوي !3 = 6. يُظهر الفرز عبر جميع الأشكال المتغيرة أنه، في هذه الحالة، يتذبذب أحد العناصر مع فترة T، والعنصر الآخر – مع فترة 2T، أو يتذبذب كلا العنصرين مع نفس الفترة 2T. لذلك، لا يمكن أن تكون شبكة مكونة من عنصرين مصدرًا موثوقًا للفوضى.

الوصف التفصيلي للاختراع

لذلك، لضمان السلوك العشوائي، يلزم وجود شبكة تتكون من ثلاثة عناصر على الأقل. في حالة عامة، يجب أن تكون هذه العناصر مكونة من عنصرين أو ثلاثة عناصر، لأن وجود عنصر إدخال فردي يحول الشبكة إلى شبكة بها عنصرين. وفقًا لذلك، يمكن للشبكة في أي وقت أن تكون في واحدة من ثماني حالات مختلفة. مولّدِ Zhang هو بالضبط شبكة من ثلاثة عناصر. ومع ذلك، يدخل هذا المولّدِ في دورة من أربع حالات، وفقًا لنتائج تحليل الرسم البياني لتغيير الحالة لمولّدِ Zhang، بغض النظر عن الحالة الأولية، حيث يتذبذب عنصر واحد مع فترة T، والعنصران الآخران – مع فترة 2T. بالطبع، لا تستبعد هذه الحقيقة الوصول إلى الفوضى، لكنها تشير إلى حساسية الشبكة للتنفيذ والتأثير المتبادل للعناصر فيما يتعلق ببعضها البعض.

للبحث عن الشبكة المطلوبة، يمكننا على الفور تجاهل جميع الشبكات ذات الحالة المستقرة. علاوة على ذلك، يمكننا على الفور استبعاد جميع الشبكات التي تحتوي فيها الدورة على أقل من ثماني حالات، حيث تسمح هذه الشبكات بالتذبذبات والتأثيرات التبادلية. الشبكات الوحيدة المتبقية هي تلك التي تتطور عبر الحالات الثمانية. العدد الإجمالي للدورات الممكنة هو !7 = 5040، بدءًا من الحالة 000، مرورًا بجميع الحالات الممكنة، والعودة إلى الحالة 000 بعد ثماني تكرارات.

لمزيد من الدراسة، من الضروري تقديم مفهوم الارتباط التلقائي لإشارة الخرج لعنصر منطقي. أثناء تطور الشبكة، يتنقل إخراج كل عنصر خلال ثماني حالات، والتي يمكن الإشارة إليها باستخدام أرقام ثنائية مكونة من ثمانية أرقام، مثل 01010101b. لحساب الارتباط التلقائي، سنقوم بتحويل هذا الرقم سبع مرات في دورة بمقدار بت واحد (عن طريق نقل البت ذي الترتيب المنخفض إلى موضع الترتيب العالي)، مع حساب كل مرة يتطابق فيها عدد البت مع القيمة الأصلية في المواضع المقابلة. إذا وجدنا، عند المقارنة، أن جميع المواضع الثمانية مختلفة، فإن هذه الإشارة ترتبط تمامًا كما هو الحال عندما تتطابق جميع المواضع الثمانية. سيكون الحد الأدنى من الارتباط هو الحال مع

أربع مطابقات وأربع اختلافات. يتم تعريف الارتباط الكلي على أنه مجموع سبع قيم مطلقة للفرق بين عدد المطابقات و4، مقسومًا على النصف، نظرًا لأن هذا المجموع دائمًا ما يكون زوجيًا.

بالنسبة لبعض التسلسلات، يكون الارتباط التلقائي الصفري ممكنًا بالفعل. ومع ذلك، في مثل هذه التسلسلات، يختلف عدد الأصفار والآحاد، وفي حالة مرور شبكة عبر دورة كاملة من الحالات الثمانية، يجب أن يكون لكل عنصر نفس عدد الحالات التي بها آحاد وأصفار عند الإخراج. من بين كل هذه التسلسلات، يكون الحد الأدنى للارتباط التلقائي الممكن مساويًا لاثنين. إجمالا، هناك أربع تسلسلات أساسية فقط مع مثل هذا الارتباط الذاتي: 00010111b، 00011011b، 00100111b، و00101011b. جميع التسلسلات الأخرى ذات أقل ارتباط تلقائي ممكن هي مشتقاتها الناجمة عن الإزاحية الدورية والعكس.

بالنسبة للشبكة المكونة من ثلاثة عناصر، يكون الحد الأدنى الممكن نظريًا للارتباط التلقائي الإجمالي هو 6، والحد الأقصى هو 26. يحتوي العداد الثنائي المكون من ثلاثة بتات على ارتباط تلقائي من 18، وعندما يتم تنفيذ ABN المقابل، لا يحدث سلوك عشوائي مطلقًا في مثل هذه الشبكة.

هناك إجمالي 648 شبكة مختلفة طوبولوجيًا، والتي تمر عبر دورة كاملة لجميع الحالات الثمانية. من بينها، 216 شبكة بها أقل ارتباط تلقائي إجمالي ممكن يبلغ 6. من هذه الشبكات، من الضروري تجاهل تلك التي ترتبط فيها إشارات خرج عنصرين مختلفين ببعضهما البعض. من الممكن نظريًا إجراء تعديل طوري لعملية العنصر في مثل هذه الشبكات، مما يؤدي إلى ترتيب الإشارة. بل إن هناك هذه الشبكات التي ترتبط فيها الإشارات ببعضها البعض على العناصر الثلاثة جميعها. وهذه الشبكات خطيرة بشكل خاص. 80 شبكة فقط، من بين الشبكات المختارة، ليس لها علاقة ارتباطية بين إشارات العناصر. نظرًا لأننا نبحث عن أصغر شبكة ممكنة، سنعطي الأفضلية للشبكات التي تحتوي على عناصر ثنائية المدخلات. لا يوجد سوى 24 من هذه الشبكات.

هناك ظرف واحد أكثر أهمية لصالح العناصر ثنائية المدخلات. لا يمكن التحكم في جميع المولّدات التي تم النظر فيها سابقًا بحيث أنه لا يمكن ربط أي إشارة خارجية مزعزعة للاستقرار من أجل فرض حدوث الفوضى والسماح للشبكات بالتتالي مع بعضها البعض. يجب أن تؤدي إضافة مدخل إضافي إلى تحويل شبكة إلى أخرى، وهو ما يلبي أيضًا المعايير المحددة تمامًا. يمكن تحقيق ذلك بسهولة أكبر عن طريق إضافة مُدخل ثالث إلى العناصر ثنائية المدخلات. نظرًا لأن العناصر ثنائية المدخلات لا يمكن أن تكون سوى بوابات XOR أو XNOR، فإن إضافة مدخل جديد لا يمكن تحقيقه إلا من خلال الحصول على بوابات XOR وXNOR ثلاثية المدخلات. في هذه الحالة، عندما يتم توفير منطق واحد للمدخل الثالث، تخضع بوابات XOR وXNOR ثنائية المدخلات لتحويل متبادل.

اتضح أنه من بين الشبكات الأربعة والعشرين المتبقية، يمكن إعادة تشكيل ثماني شبكات فقط بهذه الطريقة مع تغيير طبيعة التوليد والحفاظ على جميع الخصائص الأساسية. علاوة على ذلك، تتمتع هذه الشبكات أيضًا بمستوى قياسي منخفض من التعقيد؛ وكل شبكة من هذه الشبكات بها عنصرين من المدخلات. تم تجميع كل هذه الشبكات الثمانية في أزواج في أربع شبكات قابلة لإعادة التكوين، تتكون كل منها من ثلاثة عناصر منطقية ثلاثية المدخلات. تتوافق كل شبكة قابلة لإعادة التكوين مع شبكتين أصليتين. هذه الشبكات الأربع متكافئة وظيفيًا تمامًا، ولكن من بينها شبكة واحدة لها خاصية فريدة؛ وجميع عناصرها المنطقية متماثلة فيما يتعلق بالمدخلات المخصصة (تكون مدخلات العناصر متكافئة)، مما يبسط تنفيذ الشبكة ويسمح بتجنب الأخطاء.

وتكون هذه الشبكات المنطقية الأربعة هي جوهر الاختراع. وهي تلبي جميع المتطلبات المذكورة أعلاه ولها خاصية تعديل إضافية. وكلها تتكون من ثلاثة عناصر منطقية: بوابتا 3-XOR أو 3-XNOR، وبوابة مخرجات ثلاثية المدخلات مع دالة خاصة أكثر تعقيدًا تسمى "آحاد العد". هذه الشبكات الأربع متطابقة تمامًا بحيث ترتبط فيها العناصر ببعضها البعض، وتختلف فقط حسب نوع العناصر المستخدمة. يتم دمجها في مجموعتين: "أ" و"ب". تستخدم المجموعة "أ" نفس العناصر، سواء بوابات 3-XOR أو 3-XNOR. تستخدم المجموعة "ب" عنصرين مختلفين؛ أحدهما 3-XOR والآخر 3-XNOR. يظهر الرسم التخطيطي المنطقي لجميع هذه الشبكات في الرسومات المرفقة أدناه.

يمكن وصف عنصر "آحاد العد" على النحو التالي: يتم ضبط مخرج العنصر على 1 إذا لم يكن هناك أكثر من مدخل يساوي 1، وإلا كان المخرج صفرًا. وبالتالي، إذا كانت المدخلات الثلاثة صفرًا، فإن المخرج يكون أيضًا واحدًا منطقيًا (انظر الجدول 1).

الجدول 1. الجدول الحقيقي للعنصر المنطقي الثالث ("آحاد العد").

المدخل 3	المدخل 2	المدخل 1	المخرج
صفر	صفر	صفر	1
صفر	صفر	1	1
صفر	1	صفر	1
صفر	1	1	صفر
1	صفر	صفر	1
1	صفر	1	صفر
1	1	صفر	صفر
1	1	1	صفر

اعتمادًا على إصدار الشبكة، يمكن عكس مدخلين أو اثنين لهذا العنصر. يتم تغذية الإشارات من جميع العناصر المنطقية الثلاثة إلى مدخلات عنصر "آحاد العد". يتلقى المدخلان للبوابة الأولى XOR/XNOR إشارة من نفس البوابة ومن بوابة XOR/XNOR أخرى. يتلقى المدخلان للبوابة الثانية XOR/XNOR الثانية إشارة من بوابة XOR/XNOR الأولى ومن مخرج عنصر "آحاد العد". يتم دمج المدخلات الحرة المتبقية لكل من بوابات XOR/XNOR معًا وتمثل مدخل التعديل للشبكة المنطقية.

كل شبكة من الشبكات المنطقية الموصوفة هي الكتلة الأساسية المستخدمة لبناء مولد رقم عشوائي. سوف نسمي هذه الكتلة الأساسية "مذبذب عشوائية". وهي تشتمل على مخرج ومدخل تعديل. لا يستطيع مولّدِ الذبذبات العشوائية تعديل نفسه. من السهل التحقق من أنه مع مثل هذا التعديل، تتدهور حالة مولّدِ الذبذبات العشوائية إلى مذبذب عادي أو مصدر مستقر المستوى. علاوة على ذلك، لا يُنصح بترك مولّدِ الذبذبات العشوائية بدون تعديل على الإطلاق، لأنه نظرًا لخصائص التطبيق الفيزيائي، يمكن أن يكون سلوك مولّدِي الذبذبات اللذين بدون تعديل مختلفًا تمامًا. من المستحسن استخدام كتلة من مولّدِات الذبذبات التي تعدل بعضها البعض، ومن المستحسن أن تكون الحلقة المتكونة من التعديل كبيرة بقدر الإمكان لتقليل الارتباط المتبادل للمذبذبات.

من الناحية النظرية، يمكن التقاط الإشارة من مذبذب غير معدَّل من أي من العناصر المنطقية الثلاثة. ومع ذلك، لتقليل الارتباط المتبادل للإشارة من مولّدِات الذبذبات المختلفة، يجب التقاط الإشارة العشوائية من عنصر "آحاد العد".

دائمًا ما تكون الشبكة المنطقية ذاتية التحكم في حالة تذبذب عشوائي يتطلب طاقة. لإيقاف التوليد، يجب تعديل الشبكة بطريقة تضمن، بغض النظر عن الحالة الأولية، الوصول إلى الحالة الحتمية الوحيدة الممكنة. بالنسبة للشبكات المذكورة أعلاه، لا يمكن تحقيق ذلك عن طريق إيقاف تشغيل عنصر منطقي واحد فقط. يجب إيقاف تشغيل عنصرين على الأقل، وفي أفضل الأحوال، سيكون هذان العنصران نفس عناصر الإدخال XOR أو XNOR. يمكن إيقاف تشغيل الشبكة عن طريق دفع مخرجات هذه العناصر إلى التبديل إلى صفر أو 1. في هذه الحالة، إذا تم تعيين مخرجات عناصر XOR/XNOR على صفر، فسيكون مخرج الشبكة 1 والعكس صحيح.

لا يمكن استخدام مولّدِ الذبذبات العشوائية نفسه كمولّدِ للأرقام العشوائية، نظرًا لأنه يحتوي فقط على إخراج غير متزامن، والذي يحتوي على إشارة تناظرية عشوائية ذات نطاق عريض. يجب وضع كل مذبذب عشوائية، بغض النظر عن هيكله الداخلي، في "غلاف" متزامن يؤدي وظيفتين في وقت واحد. من ناحية، يوفر إشارة خرج منطقية مستقرة، ومن ناحية أخرى، يخزن الحالة السابقة، والتي، إذا رغبت في ذلك، يمكن استخدامها من خلال مدخلات التعديل كـ "قيمة أولية" للحصول على

الرقم العشوائي التالي. يتم عرض التعيين والرسم التخطيطي الداخلي لمثل مولّدِ الذبذبات العشوائية المتزامنة (SCO) المذكورة في الرسومات أدناه.

يحتوي SCO على مدخلات ساعة وتعديل ومخرجين: أحدهما متزامن (يُستخدم للحصول على رقم عشوائي) والآخر غير متزامن (مطلوب لتعديل مولّدات SCO الأخرى). على طول كل إشارة ساعة، يلتقط مشغل D قيمة الإشارة غير المتزامنة. يتم تغذية القيمة التي تم الحصول عليها إلى الخرج المتزامن أو، من ناحية أخرى، يمكن استخدامها للتعديل مع إشارة خارجية باستخدام بوابة XOR ثنائية المدخلات. يعتمد مولد الرقم العشوائي على كتل SCO المذكورة.

على الرغم من التعديل المتبادل، يمكن أن يكون لكتل SCO انحياز في التوزيع بين عدد الأصفار والآحاد عند المخرجات، بمعنى أكثر تحديدًا، أنه من المرجح أن يظهر نوع واحد من القيمة عند المخرجات أكثر من غيره. يرجع هذا أيضًا إلى خصائص التشغيل الفيزيائي للعناصر المنطقية للدائرة. للقضاء على هذا الانحياز، قد يلزم إجراء ما يسمى "التبييض" للأرقام العشوائية التي تم الحصول عليها.

وبالتالي، يتعلق جوهر الاختراع بشبكة منطقية ذاتية التحكم رقمية متذبذبة على نحو عشوائي تتضمن ثلاثة عناصر منطقية مرتبطة ببعضها البعض، اثنان منها عبارة عن بوابتين " Exclusive OR" و/أو "Exclusive NOR"، والعنصر المنطقي الثالث يحتوي على ثلاث مدخلات ومخرج واحد، ويقوم بتنفيذ دالة "آحاد العد" منطقية خاصة، وفيها يتم ضبط مخرجها على واحد منطقي إذا كان الواحد المنطقي موجودًا فيما لا يزيد عن أحد مدخلاتها، وإلا فسيتم ضبطه على الصفر المنطقي.

نظرًا لهذه الخصائص المفضلة، يصبح من الممكن الحصول على أرقام عشوائية حقيقية خلال فترة زمنية قصيرة جدًا باستخدام مولّدِ يتكون من ثلاثة عناصر فقط.

هناك تجسيد مفضل للجهاز، حيث يتم ربط مخرج العنصر المنطقي الأول ثنائي المدخلات بالمدخل الأول للعنصر المنطقي الثاني ثنائي المدخلات والمدخل الثاني لعنصر "آحاد العد" المنطقي الثالث، ويتم ربط مخرج العنصر المنطقي الثاني ثنائي المدخلات بمدخله الثاني والمدخل الثاني للعنصر المنطقي الأول ثنائي المدخلات والمدخل الثالث لعنصر "آحاد العد" المنطقي الثالث، ويتم ربط مخرج عنصر "آحاد العد" المنطقي الثالث بمدخله الأول والمدخل الأول للعنصر المنطقي الأول ثنائي المدخلات ومخرجات الشبكة بأكملها.

نظرًا لهذه الخصائص المواتية، يصبح من الممكن ضمان السلوك العشوائي للشبكة المنطقية ذاتية التحكم، والتي تعد أساس مولد الرقم العشوائي الحقيقية.

يوجد تجسيد آخر للجهاز، يتم فيه عكس المدخلات الثانية و/أو الثالثة للعنصر المنطقي الثالث "آحاد العد".

نظرًا لهذه الخصائص المواتية، يصبح من الممكن توفير تنفيذ محدد لمولد الرقم العشوائي الحقيقي.

يوجد تجسيد آخر للجهاز، حيث تحتوي كل من بوابات "Exclusive OR" و/أو "NOR Exclusive" ثنائية المدخلات على مدخلات منطقية ثالثة إضافية، والتي يتم دمجها معًا وربطها بمدخل تعديل خارجي إضافي لشبكة منطقية ذاتية التحكم رقمية متذبذبة على نحو عشوائي.

نظرًا لهذه الخصائص المواتية، يصبح من الممكن تحسين الخصائص الإحصائية لمولد الرقم العشوائي الحقيقية.

بالإضافة إلى ذلك، هناك تجسيد للجهاز، حيث يتضمن المولّدِ مدخل إيقاف تشغيل، بينما تحتوي كل من بوابات "Exclusive OR" و/أو "Exclusive NOR" ثنائية المدخلات على مدخلات إيقاف تشغيل إضافية مع إمكانية التبديل القسري لمخرجات كلتا البوابتين المذكورتين إلى حالة الصفر المنطقي أو الواحد المنطق بغض النظر عن حالة المدخلات الأخرى، ويتم دمج المدخلات المذكورة معًا وربطها بمدخل إيقاف تشغيل المولّدِ المحدد.

نظرًا لهذه الخصائص المواتية، يصبح من الممكن تشغيل وإيقاف تشغيل مولد الرقم العشوائي الحقيقية.

يوجد تجسيد آخر للجهاز، حيث يتم دمج الشبكة المنطقية الرقمية ذاتية التحكم المتذبذبة على نحو عشوائي بمشغل D في كتلة مذبذب عشوائية متزامنة بها مدخل ساعة مرتبط بمدخل الساعة للمشغل D، مدخل تعديل مرتبط بإدخال التعديل للشبكة المنطقية ذاتية التحكم، ومخرج غير متزامن مرتبط بإخراج الشبكة المنطقية ذاتية التحكم، ومخرج متزامن مرتبط بإخراج المشغل D، بينما يتم ربط مخرج الشبكة المنطقية ذاتية التحكم بإدخال بيانات المشغل D.

نظرًا لهذه الخصائص المواتية، يصبح من الممكن ربط مولد الرقم العشوائي الحقيقية بالدوائر الخارجية المُسجلة للوقت.

بالإضافة إلى ذلك، هناك تجسيد للجهاز، والذي يشتمل على عنصر "Exclusive OR" و/أو "Exclusive NOR" ثنائي المدخلات، والمدخل الأول مرتبط بدخل التعديل الخارجي، والمدخل الثاني مرتبط بخرج المشغل D، والخرج مرتبط بإدخال التعديل للشبكة المنطقية ذاتية التحكم.

نظرًا لهذه الخصائص المواتية، يصبح من الممكن تحسين الخصائص الإحصائية لمولد الرقم العشوائي الحقيقية عن طريق تغيير حالته الأولية.

أخيرًا، هناك تجسيد للجهاز، والذي يشتمل على مجموعة من الكتل N من مولّدات الذبذبات العشوائية المتزامنة مجتمعة في بنية حلقة، يتم دمج مدخلات الساعة معًا وربطها بإشارة ساعة

مشتركة، ويتم ربط مخرجاتها المتزامنة بخرج N-bit للمولّدِ، ومجموعة من بوابات N الإضافية ثنائية المدخلات "Exclusive OR" و/أو "Exclusive NOR" بحيث يتم ربط خرج كل بوابة بإدخال التعديل الخاص بالكتلة المقابلة لمولّدِ الذبذبات العشوائية المتزامنة، يتم ربط مدخله الأول بالإخراج غير المتزامن لكتلة مولّدِ الذبذبات العشوائية المتزامنة السابق في السلسلة، ويتم ربط المدخل الثاني بالإخراج غير المتزامن لكتلة مولّدِ الذبذبات العشوائية المتزامنة اللاحقة في السلسلة.

نظرًا لهذه الخصائص المواتية، يصبح من الممكن إنشاء أرقام عشوائية حقيقية متعددة البتات.

إن توليفة السمات الجوهرية للاختراع المقترح غير معروفة من خلال حالات المجال السابق فيما يتعلق بالطرق التي لها غرض مماثل، مما يجعل من الممكن استنتاج أنه تم استيفاء معيار الجدة فيما يتعلق بالطريقة. بالإضافة إلى ذلك، هذا الحل ليس واضحًا للمهرة في المجال.

الوصف المختصر للرسومات

من الممكن أن تتضح السمات والمزايا المميزة الأخرى لهذا الاختراع بوضوح من خلال الوصف المقدم أدناه لأغراض التوضيح، دون الحصر، باستخدام الإشارات إلى الرسومات المصاحبة، حيث:

- يوضح الشكل 1 مخططًا وظيفيًا للشبكة المنطقية ذاتية التحكم وفقًا للاختراع؛
- يوضح الشكل 2 بنية منطقية للشبكة المنطقية ذاتية التحكم باستخدام عناصر XOR وفقًا للاختراع؛
- يوضح الشكل 3 بنية منطقية للشبكة المنطقية ذاتية التحكم باستخدام عناصر XNOR وفقًا للاختراع؛
- يوضح الشكل 4 البنية المنطقية للشبكة المنطقية ذاتية التحكم باستخدام عناصر XOR وانعكاس المدخلات لعنصر "آحاد العد" وفقًا للاختراع؛
- يوضح الشكل 5 البنية المنطقية للشبكة المنطقية ذاتية التحكم باستخدام عناصر XNOR وانعكاس الإدخال لعنصر "آحاد العد" وفقًا للاختراع؛
- يوضح الشكل 6 بنية منطقية للشبكة المنطقية ذاتية التحكم باستخدام عناصر XOR وXNOR وفقًا للاختراع؛
- يوضح الشكل 7 بنية منطقية للشبكة المنطقية ذاتية التحكم باستخدام عناصر XNOR وXOR وفقًا للاختراع؛
- يوضح الشكل 8 بنية منطقية للشبكة المنطقية ذاتية التحكم باستخدام عناصر XOR وXNOR وانعكاس الإدخال لعنصر "آحاد العد" وفقًا للاختراع؛

- يوضح الشكل 9 بنية منطقية للشبكة المنطقية ذاتية التحكم باستخدام عناصر XNOR وXOR وانعكاس الإدخال لعنصر "آحاد العد" وفقًا للاختراع؛

- يوضح الشكل 10 بنية منطقية للشبكة المنطقية ذاتية التحكم ذات مدخل تعديل وفقًا للاختراع؛

- يوضح الشكل 11 بنية منطقية للشبكة المنطقية ذاتية التحكم ذات مدخل تعديل وتوليد ممكّن وفقًا للاختراع،

- يوضح الشكل 12 تخطيطًا مولّدِ الذبذبات العشوائية المتزامنة بناءً على الشبكات المنطقية الموصوفة وفقًا للاختراع،

- يوضح الشكل 13 تعيين مولّدِ الذبذبات العشوائية المتزامنة وفقًا للاختراع؛

- يوضح الشكل 14 متغيرًا لمولّدِ الذبذبات العشوائية المتزامنة باستخدام القيمة السابقة كقيمة أولية وفقًا للاختراع؛ و

- يوضح الشكل 15 مخططًا لمولد الرقم العشوائي على أساس مذبذب عشوائية متزامنة وفقًا للاختراع.

المؤشرات على الرسومات كما يلي:

1 - العنصر المنطقي الأول؛

2 - العنصر المنطقي الثاني؛

3 - العنصر المنطقي الثالث؛

4 - البوابة XOR؛

5 - البوابة XNOR؛

6 - مولّدِ الذبذبات العشوائية المتزامنة؛

7 - مولّدِ الذبذبات العشوائية؛

8 - المشغل D؛

التعديل - مدخل التعديل؛

تمكين - تمكين مدخل التوليد؛

Out - المخرج؛

Sync out - المخرج المتزامن؛

Async out - المخرج غير المتزامن؛

Clock - إشارة الساعة.

وفقًا للأشكال 1-15، يشتمل مولد الرقم العشوائي الحقيقية الذي يشتمل على شبكة منطقية ذاتية التحكم رقمية متذبذبة بشكل عشوائي كمصدر للإنتروبيا على ما يلي. تتضمن شبكة منطقية ذاتية التحكم رقمية متذبذبة على نحو عشوائي ثلاثة عناصر منطقية: 1 - أول، 2 - ثانٍ، و3 - ثالث، مرتبطين ببعضهم البعض، اثنان منهما (1 و2) يمثلان بوابات "Exclusive OR" و/أو "NOR Exclusive" ثنائية المداخل، ويشتمل العنصر المنطقي الثالث (3) على ثلاث مدخلات (يتم تحديد جميع العناصر المنطقية بواسطة الأرقام الرومانية I وII وIII) ومخرج واحد.

ينفذ العنصر المنطقي 3 دالة "آحاد العد" منطقية خاصة، حيث يتم تعيين مخرج خاص بها إلى واحد منطقي إذا كان الواحد المنطقي موجودًا في ليس أكثر من أحد مدخلاته، وإلا سيتم تعيينه على الصفر المنطقي.

يُفضل ربط العنصر المنطقي ثنائي المدخلات 1 بالمدخل الأول للعنصر المنطقي الثاني 2 ثنائي المدخلات والمدخل الثاني لعنصر "آحاد العد" المنطقي الثالث 3. يتم ربط مخرج العنصر المنطقي الثاني 2 ثنائي المدخلات بمدخله الثاني، وبالمدخل الثاني للعنصر المنطقي الأول 1 ثنائي المدخلات، وبالمدخل الثالث لعنصر "آحاد العد" المنطقي الثالث 3. يتم ربط مخرج عنصر "أحاد العد" المنطقي الثالث 3 بمدخله الأول، وبالمدخل الأول للعنصر المنطقي الأول 1 ثنائي المدخلات، وبخرج الشبكة بأكملها.

يمكن عكس المدخلات الثاني و/أو الثالث لعنصر "آحاد العد" المنطقي الثالث 3.

في تجسيد معين للاختراع، تحتوي كل من البوابات ثنائية المدخلات 1 و2 ("OR Exclusive" و/أو "Exclusive NOR") على مدخلات منطقية ثالثة إضافية، والتي يتم دمجها معًا وربطها بمدخل تعديل خارجي إضافي لشبكة منطقية ذاتية التحكم رقمية متذبذبة على نحو عشوائي (انظر الشكل 10).

في تجسيد معين للاختراع، يكون للمولّدِ مدخل إيقاف التشغيل، وتشتمل كل من بوابات "OR Exclusive" و/أو "Exclusive NOR" على مدخلات إيقاف تشغيل إضافية مع إمكانية التبديل القسري لمخرجات كلتا البوابتين المذكورين إلى حالة الصفر المنطقي أو الواحد المنطقي بغض النظر عن حالة المدخلات الأخرى، ويتم دمج هذه المدخلات معًا وربطها بمدخل إيقاف تشغيل المولّدِ المحدد (انظر الشكل 11).

على وجه الخصوص، يمكن دمج شبكة منطقية ذاتية التحكم رقمية متذبذبة على نحو عشوائي مع مشغل D في كتلة مذبذب عشوائية متزامنة مع مدخل الساعة المرتبط بمدخل الساعة للمشغل D، ومدخل تعديل مرتبط بمدل التعديل للشبكة المنطقية ذاتية التحكم، ومخرج غير متزامن مرتبط بمخرج

الشبكة المنطقية ذاتية التحكم، ومخرج متزامن مرتبط بإخراج مشغل D، بينما يتم ربط مخرج الشبكة المنطقية ذاتية التحكم بدخل بيانات المشغل D (انظر الأشكال 12-13).

في تجسيد خاص للاختراع، يشتمل المولّدِ على بوابة إضافية ثنائية المدخلات "OR Exclusive" و/أو بوابة "Exclusive NOR"، حيث يرتبط المدخل الأول منها بمدخل التعديل الخارجي، ويتم ربط المدخل الثاني بمخرج المشغل D، ويتم ربط الخرج بدخل التعديل للشبكة المنطقية ذاتية التحكم (انظر الشكل 14).

في تجسيد معين، يشتمل الاختراع على مجموعة من الكتل N لمولّدات الذبذبات العشوائية المتزامنة مجتمعة في بنية حلقة، يتم دمج مدخلات الساعة معًا وربطها بإشارة ساعة مشتركة، ويتم ربط مخرجاتها المتزامنة بخرج N-bit للمولّدِ، ومجموعة من بوابات N الإضافية ثنائية المدخلات "Exclusive OR" و/أو بوابة "Exclusive NOR" بحيث يتم ربط خرج كل بوابة بمدخل التعديل للكتلة المقابلة لمولّدِ الذبذبات العشوائية المتزامنة، ويتم ربط مدخله الأول بالخرج غير المتزامن لكتلة مولّدِ الذبذبات العشوائية المتزامنة السابقة في السلسلة، ويتم ربط المدخل الثاني بالخرج غير المتزامن لكتلة مولّدِ الذبذبات العشوائية المتزامنة اللاحقة في السلسلة (انظر الشكل 15).

وصف الاختراع

يعمل مولد الرقم العشوائي الحقيقية على النحو التالي. سنقدم المثال الأكثر شمولًا لتنفيذ الاختراع مع إدراك أن هذا المثال لا يحد من تطبيق الاختراع.

تتكون الشبكة المنطقية الرقمية ذاتية التحكم المتذبذبة على نحو عشوائي من ثلاثة عناصر منطقية مرتبطة ببعضها البعض، واثنان منها يمثلان بوابتين ثنائيتي المدخلات "Exclusive OR" و/أو بوابة "Exclusive NOR"، ويُستخدم العنصر المنطقي الثالث لتنفيذ دالة "آحاد العد" منطقية خاصة، حيث يتم ضبط مخرجها على واحد منطقي إذا كان واحد منطقي موجودًا في أكثر من أحد مدخلاتها، وإلا فإنه يتم ضبطه على صفر منطقي.

يتم تكوين مذبذب عشوائية متزامنة (SCO)، والذي يحتوي على مدخلات ساعة وتعديل ومخرجين - خرج متزامن يُستخدم للحصول على رقم عشوائي وخرج غير متزامن مطلوب لتعديل كائنات SCO الأخرى. على طول كل إشارة ساعة، يلتقط مشغل D قيمة الإشارة غير المتزامنة. يتم تغذية القيمة التي تم الحصول عليها إلى الخرج المتزامن، ومن ناحية أخرى، يتم استخدامها للانعكاس الشرطي لإشارة تعديل الدخل باستخدام بوابة XOR ثنائية المدخلات.

تم إنشاء مولد الرقم العشوائي على مثل هذه الكتل SCO.

يتم إنشاء مولد رقم عشوائي حقيقي متعدد البتات وفقًا لدائرة، والتي يتم فيها استخدام حلقة من كتل SCO، والتي يتم تعديلها في اتجاهين متعاكسين. يتلقى دخل التعديل لكل كتلة SCO إشارة من بوابة "Exclusive OR"، والتي ترتبط مدخلاتها بالمخرجات غير المتزامنة لكتل SCO السابقة واللاحقة في الحلقة.

قابلية التطبيق الصناعي

يمكن تحقيق مولد الرقم العشوائي الحقيقي المقترح عمليًا من قبل أولئك المهرة في المجال، وبمجرد تنفيذه، سيوفر تحقيق الغرض المعلن، مما يجعل من الممكن استنتاج أنه تم الوفاء بمعيار التطبيق الصناعي للاختراع.

وفقًا للاختراع المقترح، تم إنتاج نموذج أولي لمولد رقم عشوائي حقيقي. أثناء الدراسة، تم اختبار كل من مولّدات Zhang وRosin المذكورة بالفعل وكذلك المولّدِ المستند إلى الشبكة المنطقية الموصوفة بشكل تجريبي في PLIC. تم تأكيد الطبيعة العشوائية لأرقام المولّدِ المقترح من خلال التجربة التالية، والتي أُجريت باستخدام PLIC التالي: Altera Cyclone IV EP4CE22F17C6N. الشبكة في حالة "إعادة تعيين"، أي يتم تعيين مخرجات جميع العناصر المنطقية على حالة محددة مسبقًا من "صفر". بعد ذلك، في دورة ساعة واحدة، تتم إزالة إشارة إعادة الضبط، وفي دورة الساعة التالية، يتم التقاط حالة خرج مولّدِ الذبذبات العشوائية. اجتازت البيانات التي تم الحصول عليها أثناء إعادة تشغيل الشبكة المتعددة اختبار العشوائية ولم تظهر ارتباطًا كبيرًا مع بعضها البعض عند ساعة يصل إلى 150 ميجا هرتز، مما يشير إلى بداية الفوضى في أقل من 7 نانو ثانية. بعد إجراء التبييض، اجتازت الأرقام العشوائية الناتجة اختبارات العشوائية NIST.

وبالتالي، أظهر اختبار النموذج الأولي لمولد رقم عشوائي حقيقي أن النتيجة التقنية المعلنة قد تحققت (بمعنى أكثر تحديدًا، زيادة في معدل توليد الرقم العشوائي الحقيقي مع تقليل استهلاك الطاقة) بسبب حقيقة أن شبكة منطقية ذاتية التحكم رقمية متذبذبة على نحو عشوائي تتضمن ثلاثة عناصر منطقية مرتبطة ببعضها البعض، اثنان منهما يمثلان بوابتين "Exclusive OR" و/أو بوابة "Exclusive NOR"، ويشتمل العنصر المنطقي الثالث على ثلاث مدخلات ومخرج واحد، وينفذ دالة "آحاد العد" منطقية خاصة، والتي يتم فيها تعيين واحد منطقي عند مخرج له إذا كان واحد منطقي موجودًا في أكثر من أحد مدخلاته، وإلا سيتم تعيين صفر منطقي.

بالإضافة إلى ذلك، فإن النتيجة التقنية للاختراع هي مجموعة من الشبكات الوحيدة الممكنة للعناصر المنطقية، ولكل منها الخصائص التالية:

1. لا تتضمن حالات مستقرة ودورات قصيرة، مما قد يتسبب في ترتيب تشغيل الشبكة واختفاء الفوضى المنطقية.

2. تحتوي إشارات الخرج لجميع العناصر على أقل ارتباط تلقائي ممكن نظريًا، مما يدفع الشبكة إلى الوقوع في سلوك عشوائي.

3. لا يوجد ارتباط بين شكل إشارات الخرج لجميع العناصر، مما يستبعد تعديل الطور المتبادل للعناصر أثناء تشغيل الشبكة.

4. تتمتع بأصغر حجم ممكن، مما يوفر أسرع معدل تراكم ممكن للفوضى بسبب حلقات الانتشار القصيرة داخل الشبكة.

5. تحتوي على مدخل تعديل خارجي يسمح بزعزعة استقرار الشبكة (وبالتالي، منع التوازن المادي) والجمع بين الشبكات في مجموعات قابلة للتوسعة باستخدام التعديل المتبادل.

بالإضافة إلى ذلك، تستخدم شبكة واحدة فقط من هذه المجموعة العناصر المنطقية، والتي تكون متناظرة الدخل.

وبالتالي، تتيح هذه الشبكات إنشاء مولد رقم عشوائي بالخصائص الفريدة التالية:

1. الأرقام الناتجة عشوائية حقًا، مما يسمح باستخدامها لأغراض التشفير.

2. معدل توليد الرقم العشوائي مرتفع للغاية بحيث لا يمكن التنبؤ بسلوك الشبكة حتى أثناء انتشار الإشارة من خلال عدة عناصر منطقية. وبالتالي، عند تنفيذها في أنظمة المعالجات الدقيقة، يمكن الحصول على رقم عشوائي في دورة ساعة واحدة. يلبي معدل التوليد المذكور أي حاجة محتملة افتراضيًا.

3. يسمح إدخال التعديل بمزيد من تحسين الخصائص، حيث يمكن تغذيتها برقم عشوائي آخر (ما يسمى بـ "قيمة أولية" لمولد الرقم العشوائي المقترَح). يفرض هذا على الشبكة أن تبدأ من حالة جديدة في كل مرة.

4. يسمح نفس الدخل بالتعديل المتبادل لبتات المولّدِ المقترح، وبالتالي زيادة معدل بدء الفوضى.

5. يجعل الحد الأدنى لحجم الشبكة المولّدِ المقترح هو الأكثر اقتصادا من حيث استهلاك الطاقة.

6. يمكن تنفيذ المولّدِ المقترح بكفاءة متساوية على كل من العناصر المنفصلة وفي PLICs أو ASICs.

7. إن تصميم المولّدِ المقترح بسيط وتكاليف تنفيذه ضئيلة، مما يجعل من الممكن استخدامه في كل مكان، بما في ذلك أجهزة منخفضة التكلفة وموفرة للطاقة.

المرجع:

[1] Maxim Semiconductors. Building a Low-Cost White-Noise Generator. Application note 3469.

[2] R. Zhang, H. L. D. de S. Cavalcante, Z. Gao, D. J. Gauthier, J. E. S. Socolar, M. M. Adams, and D. P. Lathrop. Boolean Chaos. Phys. Rev. E 80, 045202 (2009).

[3] David P. Rosin, Damien Rontani, Daniel J. Gauthier, and Eckehard Schöll. Experiments on autonomous Boolean networks. Chaos 23, 025102 (2013).

[4] Hugo L. D. de S. Cavalcante, Daniel J. Gauthier, Joshua E. S. Socolar and Rui Zhang. On the origin of chaos in autonomous Boolean networks. Phil. Trans. R. Soc. A 368, 495-513 (2010).

[5] David Rosin, Dynamics of Complex Autonomous Boolean Networks. Doctoral dissertation. Technische Universität Berlin.

عناصر الحماية

1. مولد رقم عشوائي حقيقي يشتمل على شبكة منطقية ذاتية التحكم رقمية متذبذبة على نحو عشوائي كمصدر للإنتروبيا، ويتميز بأن الشبكة المنطقية الرقمية ذاتية التحكم المتذبذبة على نحو عشوائي المذكورة تتضمن ثلاثة عناصر منطقية مرتبطة ببعضها البعض، العنصر الأول عبارة عن بوابة ثنائية المدخلات "Exclusive OR" أو "Exclusive NOR"، والعنصر الثاني عبارة عن بوابة ثنائية المدخلات "Exclusive OR" أو "Exclusive NOR"، والعنصر المنطقي الثالث يحتوي على ثلاث مدخلات ومخرج واحد، ويقوم بتنفيذ دالة "آحاد العد" منطقية خاصة، وفيها يتم ضبط مخرجها على واحد منطقي إذا كان الواحد المنطقي موجودًا فيما لا يزيد عن أحد مدخلاتها، وإلا فسيتم ضبطه على الصفر المنطقي، بينما يتم ربط مخرج العنصر المنطقي الأول ثنائي المدخلات بالمدخل الأول للعنصر المنطقي الثاني ثنائي المدخلات والمدخل الثاني لعنصر "آحاد العد" المنطقي الثالث، ويتم ربط مخرج العنصر المنطقي الثاني ثنائي المدخلات بمدخله الثاني والمدخل الثاني للعنصر المنطقي الأول ثنائي المدخلات والمدخل الثالث لعنصر "آحاد العد" المنطقي الثالث، ويتم ربط مخرج عنصر "آحاد العد" المنطقي الثالث بمدخله الأول والمدخل الأول للعنصر المنطقي الأول ثنائي المدخلات ومخرجات الشبكة بأكملها.

2. المولّدِ وفقًا لعنصر الحماية 1، حيث يتميز بأنه يتم عكس المدخلات الثانية و/أو الثالثة للعنصر المنطقي الثالث "آحاد العد".

3. المولّدِ وفقًا لأي من عناصر الحماية 1-2، حيث يتميز بأن كلا من بوابات "OR Exclusive" و/أو "Exclusive NOR" ثنائية المدخلات لها مدخلات منطقية ثالثة إضافية، والتي يتم دمجها معًا ويتم ربطها بدخل تعديل خارجي إضافي للشبكة المنطقية الرقمية ذاتية التحكم المتذبذبة على نحو عشوائي.

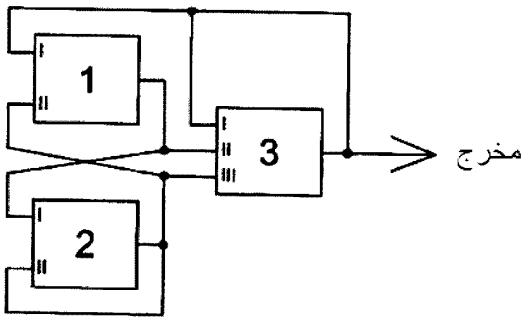
4. المولّدِ وفقًا لأي من عناصر الحماية 1-3، حيث يتميز بأن المولّدِ لديه مدخل إيقاف تشغيل، بينما تحتوي كل من بوابتي "Exclusive OR" و/أو "Exclusive NOR" على مدخلات إيقاف تشغيل إضافية مع إمكانية تبديل مخرجات كلتا البوابتين المذكورين بشكل قسري إلى حالة الصفر المنطقي أو الواحد المنطقي بغض النظر عن حالة المدخلات الأخرى، ويتم دمج هذه المدخلات معًا وربطها بمدخل إيقاف تشغيل المولّدِ المحدد.

5. المولّدِ وفقًا لأي من عناصر الحماية 3-4، حيث يتميز بأنه يتم دمج الشبكة المنطقية الرقمية ذاتية التحكم المتذبذبة على نحو عشوائي بمشغل D في كتلة مذبذب عشوائية متزامنة بها مدخل ساعة مرتبط بمدخل الساعة للمشغل D، مدخل تعديل مرتبط بمدخل التعديل للشبكة المنطقية

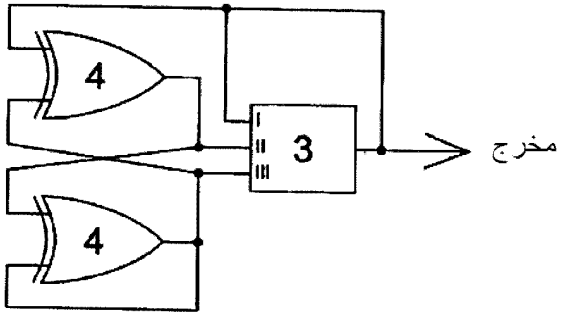
ذاتية التحكم، ومخرج غير متزامن مرتبط بإخراج الشبكة المنطقية ذاتية التحكم، ومخرج متزامن مرتبط بمخرج المشغل D، ومخرج الشبكة المنطقية ذاتية التحكم المرتبط بدخل البيانات للمشغل D.

6. المولّدِ وفقًا لعنصر الحماية 5، حيث يتميز بأن ذلك المولّدِ المذكور يشتمل على بوابة "Exclusive OR" و/أو "Exclusive NOR" إضافية ثنائية المدخلات، ويتم ربط المدخل الأول لها بمدخل التعديل الخارجي، ويتم ربط المدخل الثاني بمدخل المشغل D، ويتم ربط المخرج بمدخل التعديل للشبكة المنطقية ذاتية التحكم.

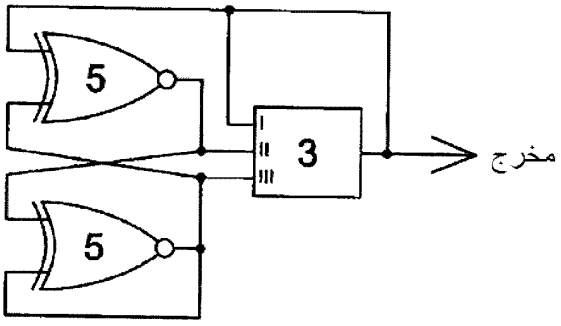
7. المولّدِ وفقًا لأي من عناصر الحماية 5-6، حيث يتميز بأنه يشتمل المولّدِ المذكور على مجموعة من الكتل N لمولّدِات الذبذبات العشوائية المتزامنة في بنية حلقة، ويتم دمج مدخلات الساعة معًا وربطها بإشارة ساعة مشتركة، ويتم ربط مخرجاتها المتزامنة بمخرج N-bit للمولّدِ، ومجموعة من بوابات "Exclusive OR" و/أو "Exclusive NOR" الإضافية ثنائية المدخلات حيث يتم ربط خرج كل بوابة بمدخل التعديل للكتلة المقابلة لمولّدِ الذبذبات العشوائية المتزامنة، ويتم ربط مدخلاته الأولى بالخرج غير المتزامن لكتلة مولّدِ الذبذبات العشوائية المتزامنة السابق في السلسلة، ويتم ربط المدخل الثاني بالخرج غير المتزامن لكتلة مولّدِ الذبذبات العشوائية المتزامنة اللاحقة في السلسلة.



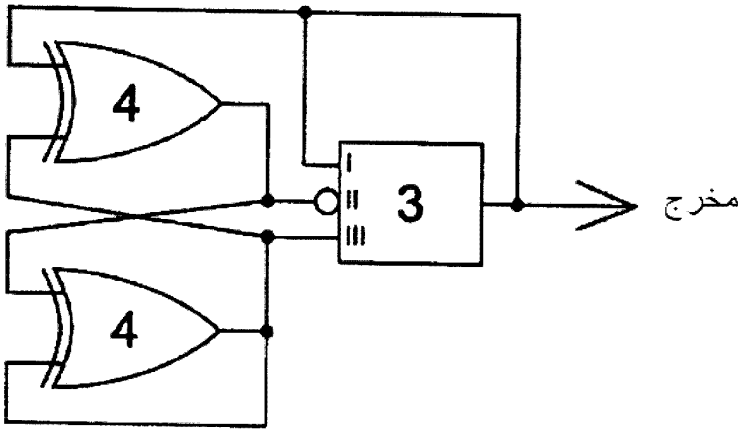
الشكل 1



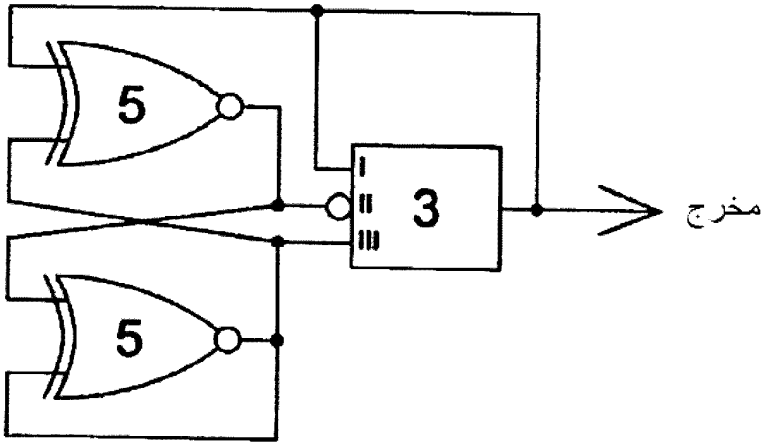
الشكل 2



الشكل 3

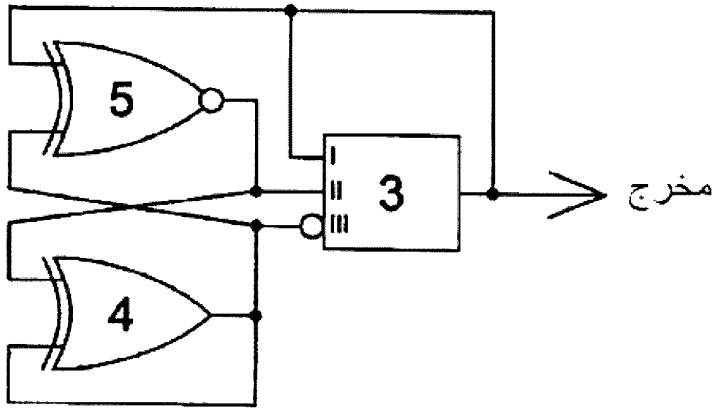


الشكل 4

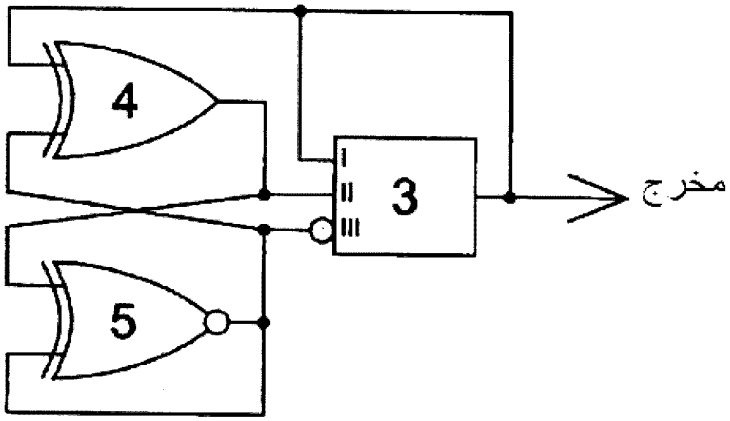


الشكل 5

32



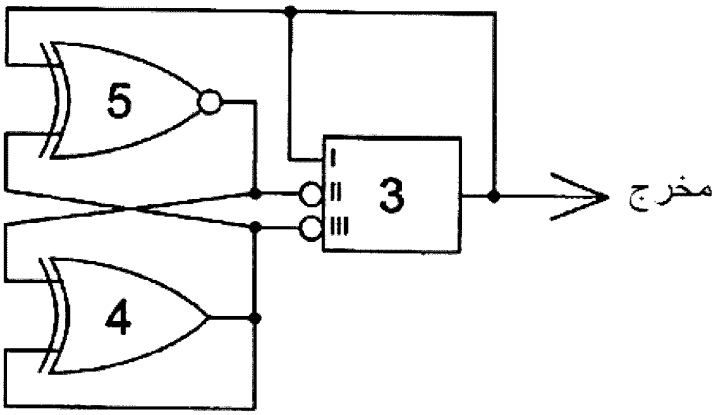
الشكل 6



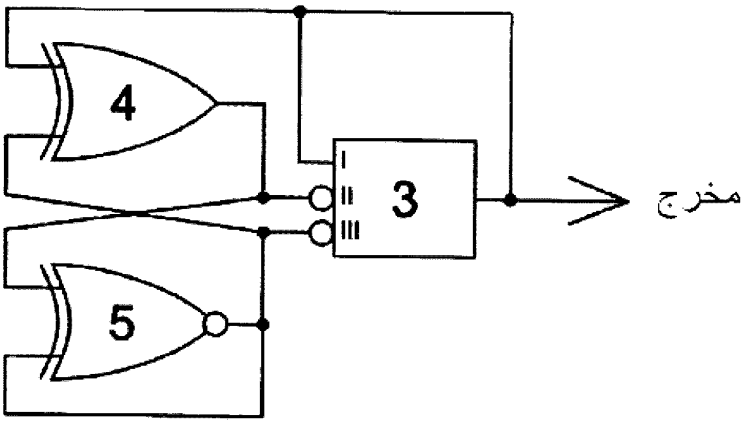
الشكل 7

33

34

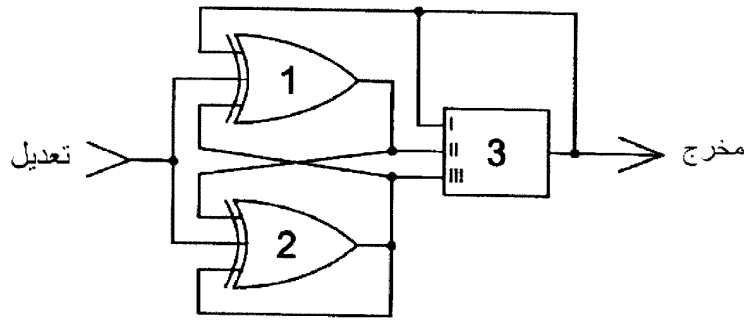


الشكل 8

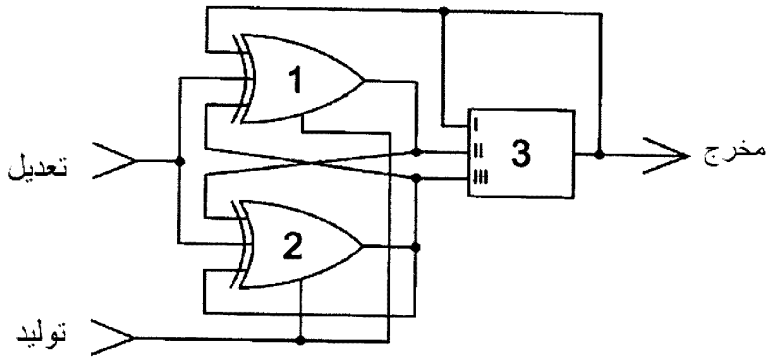


الشكل 9

38



الشكل 10



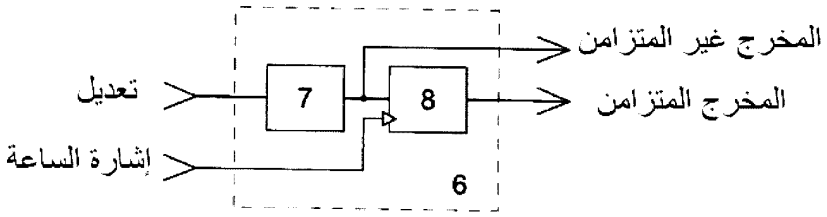
الشكل 11

39

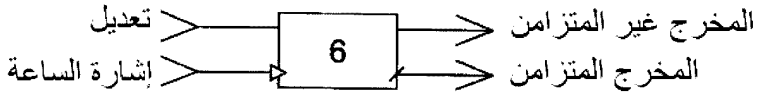
40

6/7

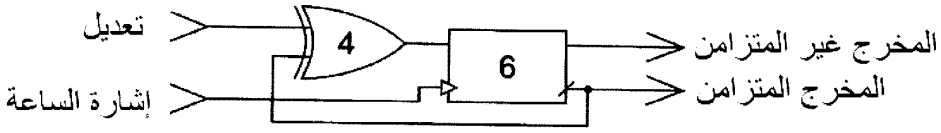
41



الشكل 12



الشكل 13



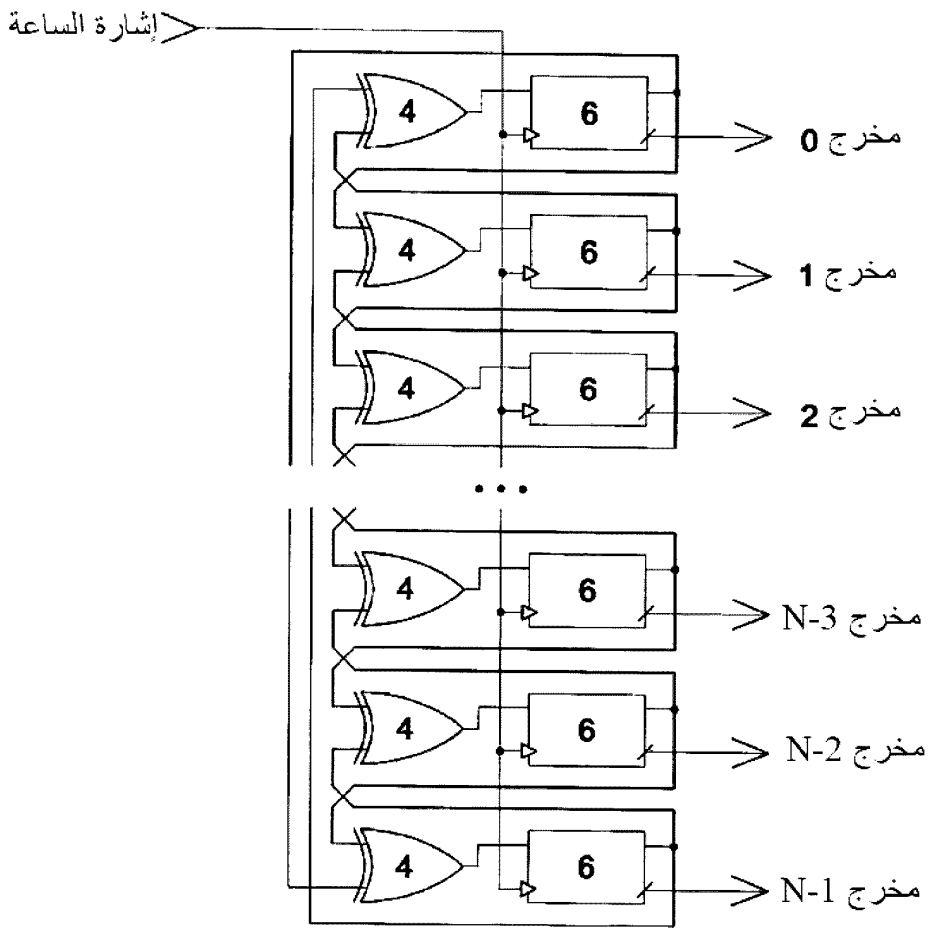
الشكل 14

42

43

7/7

44



الشكل 15

45

MA 59288B1

ROYAUME DU MAROC
OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE

OMPIC

المملكة المغربية
المكتب المغربي للملكية الصناعية و التجارية

RAPPORT DE RECHERCHE AVEC OPINION SUR LA BREVETABILITE

(Conformément aux articles 43 et 43.2 de la loi 17-97 relative à la protection de la propriété industrielle telle que modifiée et complétée par la loi 23-13)

Renseignements relatifs à la demande	
N° de la demande : 59288	Date de dépôt :18/01/2021 Date d'entrée en phase nationale : 25/01/2023 Date de priorité: 17/07/2020
Déposant : PHYSTECH TECHNOLOGIES TRUE RANDOM AG	
Intitulé de l'invention : GÉNÉRATEUR DE NOMBRES VÉRITABLEMENT ALÉATOIRES	

Le présent document est le rapport de recherche avec opinion sur la brevetabilité établi par l'OMPIC conformément aux articles 43 et 43.2, et notifié au déposant conformément à l'article 43.1 de la loi 17-97 relative à la protection de la propriété industrielle telle que modifiée et complétée par la loi 23-13.

Les documents brevets cités dans le rapport de recherche sont téléchargeables à partir du site http://worldwide.espacenet.com, et les documents non brevets sont joints au présent document, s'il y en a lieu.

Le présent rapport contient des indications relatives aux éléments suivants :

Partie 1 : Considérations générales
- ☒ Cadre 1 : Base du présent rapport
- ☐ Cadre 2 : Priorité
- ☐ Cadre 3 : Titre et/ou Abrégé tel qu'ils sont définitivement arrêtés

Partie 2 : Rapport de recherche

Partie 3 : Opinion sur la brevetabilité
- ☐ Cadre 4 : Remarques de forme et de clarté
- ☐ Cadre 5 : Défaut d'unité d'invention
- ☐ Cadre 6 : Observations à propos de certaines revendications exclues de la brevetabilité
- ☒ Cadre 7 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle

Examinateur: EL KINANI Mohamed	**Date d'établissement du rapport** : 03/03/2023
Téléphone: 212 5 22 58 64 14/00	

Partie 1 : Considérations générales

Cadre 1 : base du présent rapport

Les pièces suivantes de la demande servent de base à l'établissement du présent rapport :

- Description
  19 Pages
- Revendications
  1-7
- Planches de dessin
  7 Pages

Partie 2 : Rapport de recherche

Classement de l'objet de la demande :

CIB : G06F7/58; H03K3/84
CPC : G06F7/58 ; G06F7/588 ; H03K19/173 ; H03K19/21 ; H03K3/84

Plateformes et bases de données électroniques de recherche :

EPOQUENET, WPI, ScienceDirect, IEEE, ORBIT

Catégorie*	Documents cités avec, le cas échéant, l'indication des passages pertinents	N° des revendications visées
A	WO 2019/222866 A1; TAIYUAN UNIVERSITY OF TECHNOLOGY; 28/11/2019	1-7
A	CN 107943451 A ;UNIV XIDIAN ; 20/04/2018	1-7
A	US 2009/0327381 A 1 ; HORIZON SEMICONDUCTORS LTD ; 31/12/2009	1-7

***Catégories spéciales de documents cités :**

-« **X** » document particulièrement pertinent ; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
-« **Y** » document particulièrement pertinent ; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
-« **A** » document définissant l'état général de la technique, non considéré comme particulièrement pertinent
-« **P** » documents intercalaires ; Les documents dont la date de publication est située entre la date de dépôt de la demande examinée et la date de priorité revendiquée ou la priorité la plus ancienne s'il y en a plusieurs
-« **E** » Éventuelles demandes de brevet interférentes. Tout document de brevet ayant une date de dépôt ou de priorité antérieure à la date de dépôt de la demande faisant l'objet de la recherche (et non à la date de priorité), mais publié postérieurement à cette date et dont le contenu constituerait un état de la technique pertinent pour la nouveauté

Partie 3 : Opinion sur la brevetabilité

Cadre 7 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle

Nouveauté	Revendications 1-7 Revendications aucune	Oui Non
Activité inventive	Revendications 1-7 Revendications aucune	Oui Non
Application Industrielle	Revendications 1-7 Revendications aucune	Oui Non

Il est fait référence aux documents suivants. Les numéros d'ordre qui leur sont attribués ci-après seront utilisés dans toute la suite de la procédure

D1 : WO 2019/222866 A1

1. Nouveauté

Aucun document de l'état de la technique ne divulgue un générateur de nombres aléatoires comprenant un réseau booléen autonome numérique a oscillation chaotique comme source d'entropie tel que décrit dans la revendication 1 de la présente demande.

D'où l'objet de la revendication indépendante 1 est nouveau au sens de l'article 26 de la loi 17-97 telle que modifiée et complétée par la loi 23-13. Par conséquent, l'objet des revendications 2-7 est également nouveau.

2. Activité inventive

Le document D1 considéré comme l'état de la technique le plus proche de l'objet de la revendication indépendante 1 divulgue un générateur de nombres aléatoires comprenant un réseau booléen autonome numérique a oscillation chaotique comme source d'entropie, caractérisé en ce que ledit réseau booléen autonome numérique a oscillation chaotique comprend trois éléments logiques connectés les uns aux autres, dont le premier est un "OU exclusif" à deux entrées, le second est une porte "OU exclusif" à deux entrées.

Par conséquent, L'objet de la revendication 1 diffère de ce dispositif connu en ce le premier élément logique est un "OU exclusif" ou "NON OU exclusif" à deux entrées, le second est une porte "OU exclusif" ou "NON OU exclusif" à deux entrées, et le troisième élément logique ayant trois entrées et une sortie, et implémente une logique "comptage des uns", dans lequel un « un logique » est déterminé sur sa sortie s'il n'y a pas plus qu'une de ses entrées qui produit un « un logique », sinon il est mis à « zéro logique », tandis que la sortie des deux premiers éléments logiques d'entrée est connecté à la première entrée du second élément logique à deux entrées et à la deuxième entrée du troisième élément logique "comptage des uns", la sortie du deuxième élément logique à deux entrées est relié à sa deuxième entrée, à la deuxième entrée du premier élément logique à deux entrées, et à la troisième entrée du troisième élément

logique "comptage des uns", et la sortie du troisième élément logique "comptage des uns" est reliée à sa première entrée, à la première entrée du premier élément logique à deux entrées, et à la sortie de l'ensemble du réseau.

Le problème technique objectif que la présente invention se propose de résoudre peut donc être considéré comme augmenter la vitesse avec quels vrais nombres aléatoires peuvent être générés tout en réduisant consommation d'énergie.

La combinaison de l'ensemble ces caractéristiques n'est pas divulgué dans l'art antérieur et n'en découle pas de manière évidente.

D'où l'objet de la revendication 1 peut être considéré comme impliquant une activité inventive au sens de l'article 28 de la loi 17-97 telle que modifiée et complétée par la loi 23-13.

Les revendications 2-7 dépendent d'une ou de plusieurs revendications indépendantes dont l'objet est considéré nouveau et inventif, comme indiqué auparavant, et elles satisfont donc également, en tant que telles, aux exigences de la loi 17/97 modifiée et complétée par la loi 23-13 en matière d'activité inventive.

3. Application industrielle

L'objet de la présente invention est susceptible d'application industrielle au sens de l'article 29 de la loi 17-97 telle que modifiée et complétée par la loi 23-13, parce qu'il présente une utilité déterminée, probante et crédible.