(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5787311号
(P5787311)

(45)発行日　平成27年9月30日(2015.9.30)　(24)登録日　平成27年8月7日(2015.8.7)

(51)Int.Cl.			F I		
G06F	7/58	(2006.01)	G06F	7/58	A
G09C	1/00	(2006.01)	G09C	1/00	650B
H04L	9/10	(2006.01)	H04L	9/00	621Z

請求項の数 6　(全 17 頁)

(21)出願番号　特願2011-82473(P2011-82473)
(22)出願日　平成23年4月4日(2011.4.4)
(65)公開番号　特開2012-220968(P2012-220968A)
(43)公開日　平成24年11月12日(2012.11.12)
審査請求日　平成26年4月3日(2014.4.3)

特許法第３０条第１項適用　平成２３年３月９日　社団法人応用物理学会発行の「２０１１年春季　第５８回応用物理学関係連合講演会「講演予稿集」（ＤＶＤ－ＲＯＭ）」に発表

(73)特許権者　504182255
国立大学法人横浜国立大学
神奈川県横浜市保土ヶ谷区常盤台７９番１号
(74)代理人　100060690
弁理士　瀧野　秀雄
(74)代理人　100108017
弁理士　松村　貞男
(74)代理人　100134832
弁理士　瀧野　文雄
(74)代理人　100144277
弁理士　乙部　孝
(74)代理人　100165308
弁理士　津田　俊明

最終頁に続く

(54)【発明の名称】物理乱数発生器

(57)【特許請求の範囲】

【請求項１】

周期パルスが入力され、遅延時間揺らぎを有する出力信号を出力する第１の遅延回路と、該第１の遅延回路の前記出力信号が入力される第１入力端及び他の信号が入力される第２入力端を有し、前記第１入力端及び前記第２入力端へ入力される信号の到達時刻の時間差に応じて“１”または“０”の信号を確率的に出力する論理回路とを備えた物理乱数発生器であって、

前記他の信号と前記周期パルスとは同期関係を有し、前記論理回路は、前記出力信号の到達時刻と前記他の信号の到達時刻との時間差が所定の値（反応時間差：Ｔｈ）のときに確率５０％で“１”の信号を出力することを特徴とする物理乱数発生器。

【請求項２】

前記論理回路にＡＮＤ回路が備えられ、前記第１入力端及び前記第２入力端が前記ＡＮＤ回路の入力へ接続され、前記第１の遅延回路の遅延時間は、動作時に前記論理回路から出力される“１”の発生確率が５０％になるように設定されていることを特徴とする請求項１に記載の物理乱数発生器。

【請求項３】

前記第１の遅延回路が可変遅延回路とされることを特徴とする請求項１または２に記載の物理乱数発生器。

【請求項４】

前記第２入力端に第２の遅延回路が接続され、前記第１及び第２の遅延回路の少なくと

も一つが可変遅延回路とされることを特徴とする請求項１または２に記載の物理乱数発生器。
【請求項５】
前記第1の遅延回路は複数のＳＦＱ素子を直列接続したジョセフソン伝送路で構成され、前記ＡＮＤ回路は一つの超電導リングにＳＦＱの通過する２個の入力用と１個の出力用のジョセフソン素子を有するＳＦＱ素子を含む複数のＳＦＱ素子により構成されていることを特徴とする請求項２乃至４いずれか１項に記載の物理乱数発生器。
【請求項６】
前記論理回路がフリップフロップ回路を備えることを特徴とする請求項２乃至４いずれか１項に記載の物理乱数発生器。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、遅延回路の遅延時間の時間揺らぎに基づいて乱数を発生する物理乱数発生器であり、より詳細には、超電導単一磁束量子（Ｓｉｎｇｌｅ　Ｆｌｕｘ　Ｑｕａｎｔｕｍ、以下、「超電導ＳＦＱ」ともいう。）による遅延線の遅延時間揺らぎ（以下、「タイミングジッタ」ともいう。）に基づいて乱数を発生する物理乱数発生器に関する。
【背景技術】
【０００２】
現代の情報社会のインフラとしてネットワークが必須であり、そこではデジタル信号で情報が蓄積され配信される。この情報の安全性を確保するためのデータの暗号化等に乱数が必要とされている。乱数には、その発生方法によって疑似乱数と真性乱数がある。
【０００３】
通常は発生が容易な疑似乱数が用いられている。疑似乱数はハードウエアのレジスタと帰還用論理を組み合わせた論理回路またはソフトウエアプログラムでＣＰＵを使って予め定めた論理にしたがって発生される（特許文献１を参照）。
【０００４】
しかし、疑似乱数は、人為的に定めた論理により発生されるため発生規則が推定される可能性があり、真の暗号化には不向きである。したがって、データの取り扱いの安全性を高めるには人為的な発生規則を使わない真性乱数が好ましい。
【０００５】
真性乱数を発生するためには、本質的にランダムな自然界の現象を基にして発生される物理乱数を利用することが考えられる。物理乱数発生器としては、熱に伴う予測不可能な原子や分子の動きから生じる熱雑音を利用したものが実用化されている（特許文献２を参照）。
【０００６】
ここで、物理乱数の応用範囲として機密文章暗号化プログラムやゲーム機械さらに電子認証、数値シミュレーション（モンテカルロ法）等々の日常生活に密着した様々な使用を考慮すると、パーソナルコンピュータや携帯端末機器等で物理乱数を利用できるようにするための簡易な構成の物理乱数発生器が求められる。
【０００７】
簡易な物理乱数発生器であるためには、省電力、小型化が求められ、さらに近年のデジタル信号処理の高速化に伴って高速化が必要である。
【０００８】
上記の要求を満足するために、超電導を用いて超高速、低消費電力の単体素子で動作する乱数発生素子が研究されている（特許文献３）。
【０００９】
超電導素子として単一磁束量子素子（ＳＦＱ素子）が注目されている。ＳＦＱ素子は、超電導材からなる超電導リング（インダクタンス）と、この超電導リングの一部に設けられた、ごく薄い絶縁膜からなるジョセフソン接合とで構成されており、磁束量子を情報担

体としている。
【００１０】
ＳＦＱ素子で情報担体となる単一磁束量子（ＳＦＱ）は、量子化された磁束の最小単位（Φ_0＝ｈ／２ｅ＝２．０７×１０$^{-15}$Ｗｅｂｅｒ、ただし、ｈはプランク定数、ｅは電子の電荷）である。この単一磁束量子（ＳＦＱ）は非常に小さい物理量であり、これを情報の１ビットに対応させることで高性能な演算回路を構成することができる。
【００１１】
ＳＦＱ素子では、ＳＦＱの動きを制御するために、ジョセフソン接合とインダクタンスとを含む超電導閉ループを形成する。該閉ループで磁束量子Φ_0を保持可能にする場合には、ジョセフソン接合の臨界電流をＩｃで表すと、Ｌ・ＩｃがΦ_0の１．５倍程度になるように設計パラメータを定める。また、ＳＦＱを伝搬させる場合は、Ｌ・ＩｃがΦ_0の０．５倍程度に設計パラメータを定める。
【００１２】
このＳＦＱを情報担体とするＳＦＱ素子を用いることで、１００ギガヘルツ以上の超高速動作と、ゲートあたり数マイクロワット（μＷ）以下の低消費電力特性を特徴とする論理回路を実現することができる。
【００１３】
ここで、本願発明者は、ＳＦＱ素子が外部からの電流、磁界に対して非常に高感度であることに着目してＳＦＱ素子による超電導比較回路を用いた物理乱数発生器（以下比較器型物理乱数発生器と略記する）を開発・報告している（非特許文献１を参照）。この比較器型物理乱数発生器は、図１８に示すように、熱雑音源を直接ＳＦＱ素子による比較器に接続したもので、従来の半導体回路を用いた乱数発生器に比べると増幅器による帯域制限を受けることがない。
【００１４】
しかしながら、上記比較器型乱数発生器は、図１９に示すように、制御電流に対する１レベルの信号（以下「“１”」ともいう。）の発生確率特性の傾斜が急峻（「傾きが大きい」ともいう）で、“１”の発生確率が０から１または１から０へと変化する際の制御電流Ｉｃｔｌの差（これを「グレイゾーン幅」という。）が狭い。そのため、０レベルの信号（以下「“０”」ともいう。）と１レベルの信号の発生確率を安定に制御するためにはＳＦＱ素子の制御電流の値を精密に保持する必要がある。また、外部電圧の変動に非常に敏感で、動作が安定しないという問題があった。ここで、“０”、“１”を電圧、電流へ対応させるとき電圧の高低、電流の大小へ対応させる関係は任意である。
【先行技術文献】
【特許文献】
【００１５】
【特許文献１】特開平０９－２８２１４６号公報
【特許文献２】国際公開Ｗ０２００２／０２７２６０
【特許文献３】特開平０７－１４７４３５号公報
【非特許文献】
【００１６】
【非特許文献１】Ｙ．Ｙａｍａｎａｓｈｉ，Ｎ．　Ｙｏｓｉｋａｗａ「Ｓｕｐｅｒｃｏｎｄｕｃｔｉｖｅ　Ｐｙｈｉｓｉｃａｌ　Ｒａｎｄｏｍ　Ｎｕｍｂｅｒ　Ｇｅｎｅｒａｔｏｒ　Ｕｓｉｎｇ　Ｔｈｅｒｍａｌ　Ｎｏｉｓｅｓ　ｉｎ　ＳＦＱ　Ｃｉｒｃｕｉｔｓ」，ＩＥＥＥ　Ｔｒ．　ｏｎ　Ａｐｐｉｌｉｅｄ　Ｓｕｐｅｒｃｏｎｄｕｃｔｉｖｉｔｙ，Ｖｏｌ．　１９．Ｎｏ．３　Ｊｕｎｅ２００９
【発明の概要】
【発明が解決しようとする課題】
【００１７】
本発明は上記の問題に鑑みてなされたものであり、暗号化等で必要な高速の物理乱数を安定に発生する物理乱数発生器を提供することを目的とする。

【課題を解決するための手段】
【００１８】
本願発明者が先に開発・報告した比較器型物理乱数発生器（非特許文献１）では、ＳＦＱ素子中のジョセフソン接合を流れる電流の熱雑音による振幅方向の揺らぎを利用しているため、外部電圧の変動によりその制御電流に対する“１”の発生確率特性が変化することが問題になった。そこで、本願発明者は、振幅方向の揺らぎを直接検出するのではなく、熱による伝送路の遅延時間の時間揺らぎに基づいて物理乱数が発生することに着目し本願発明を完成した。
【００１９】
本発明に係る物理乱数発生器は、周期パルスが入力され、遅延時間揺らぎを有する出力信号を出力する第１の遅延回路と、該第１の遅延回路の前記出力信号が入力される第１入力端及び他の信号が入力される第２入力端を有し、前記第１入力端及び前記第２入力端へ入力される信号の到達時刻の時間差に応じて“１”または“０”の信号を確率的に出力する論理回路とを備えた物理乱数発生器であって、前記他の信号と前記周期パルスとは同期関係を有し、前記論理回路は、前記出力信号の到達時刻と前記他の信号の到達時刻との時間差が所定の値（反応時間差：Ｔｈ）のときに確率５０％で“１”の信号を出力することを特徴としている。ここでパルスの到達時刻とはパルス波形のピークの到達時刻として把握できる。また、パルス波形の頂上部が平坦な場合は、パルス幅の中央部の到達時刻として把握できる。
【００２０】
遅延回路は遅延素子の熱的な揺らぎにより時間方向の揺らぎ、すなわち遅延時間揺らぎを有している。この遅延時間揺らぎは遅延時間が増えるに従い増大する特性を有する。第１入力端に時間方向の揺らぎを持つ入力信号と第２入力端へ入力される基準時刻毎のパルスとを比較することにより、２つの入力に応じて“０”または“１”を出力する論理回路を使用する。遅延回路への入力に周期パルスを用いることで遅延回路の出力には時間揺らぎを伴う周期パルスが出力信号として現れる。
【００２１】
論理回路の第１入力端へ時間揺らぎを伴う周期パルスが入力され、第２入力端に遅延回路へ入力される周期パルスと同期関係を有するパルスとが入力されると、論理回路の出力は２つのパルスの入力時間の重なり具合に応じて“０”または“１”を出力する。２つのパルスの入力時間差による重なり具合は遅延時間揺らぎにより変動するが、この遅延時間揺らぎは遅延回路の熱的な揺らぎに由来するため予測ができない。
【００２２】
２つの周期パルスの論理回路への入力時間差による重なり具合が小さい場合には、論理回路の出力における“１”の発生確率は０に近くなり、２つの周期パルスがほぼ同時刻に論理回路へ入力されて２つのパルスの重なりが大きい場合には、論理回路の出力における“１”の発生確率は１に近くなる。“１”の発生確率が２つの入力パルス（以下、パルス入力ともいう）の相対的な時間差により連続的に変化する部分の特性は、遅延時間揺らぎ、パルス波形及び論理回路の入出力特性に依存している。
【００２３】
発明に係る論理回路では、遅延回路における遅延時間揺らぎにより、出力における“１”の発生確率が０から１へまたは１から０へと変化する途中の過程が緩やかになり、グレイゾーン幅がひろがるので、確率５０％で“１”を出力する２つの入力間の相対的な時間差である反応時間差（Ｔｈ）を容易に決めることができる。そして、予め遅延時間を選ぶことで２つのパルスの相対的な時間差を反応時間差Ｔｈに設定することができることから物理乱数が得られる。ここで、「確率５０％」とは、回路作製上の回路素子パラメータの誤差範囲を含む。
【００２４】
次に、請求項２に係る物理乱数発生器は、請求項１に記載の物理乱数発生器において、前記論理回路にＡＮＤ回路が備えられ、前記第１入力端及び前記第２入力端が前記ＡＮＤ

回路の入力へ接続され、前記第１の遅延回路の遅延時間は、動作時に前記論理回路から出力される“１”の発生確率が５０％になるように設定されていることを特徴としている。

【００２５】

遅延回路の遅延時間は、動作時に前記論理回路から出力される“１”の発生確率が５０％になるように設定されている。このように動作時の特性を踏まえて遅延時間を設定することで、遅延特性の非線形性やパルス波形の変形に対応することができて、パルスの周期毎にＡＮＤが行われ、“１”が出力されるか否かが遅延回路の時間揺らぎにより決められる。また、ＡＮＤ回路の出力に物理乱数が発生する。遅延時間差に伴う“１”の発生確率の変化の様子が滑らかであれば、ＡＮＤ回路へ入力される２つの信号の平均遅延時間の差は、クロック周期の自然数倍に反応時間差を加減した値付近になる。ここで、「平均遅延時間」とは、時間的に前後に揺らぐパルスの遅延時間を長時間平均した値を意味する。

【００２６】

また、請求項３に係る物理乱数発生器は、請求項１または２に記載の物理乱数発生器において、前記第１の遅延回路が可変遅延回路とされることを特徴としている。ここで、「可変遅延回路」とは、動作時に遅延時間を制御（可変）することができる遅延回路を意味する。

【００２７】

また、請求項４に係る物理乱数発生器は、請求項１または２に記載の物理乱数発生器において、前記第２入力端に第２の遅延回路が接続され、前記第１及び第２の遅延回路の少なくとも一つが可変遅延回路とされることを特徴としている。

【００２８】

可変遅延回路を用いていることから、動作時に遅延時間を制御することが可能になり、さらに、“１”の発生確率を５０％になるように遅延時間を調整することで“０”と“１”の発生確率を揃えた一様乱数にすることができる。ここで、発生確率の５０％は要求精度により決まるので実際は５０％近傍の値でも良い。

【００２９】

請求項５に係る物理乱数発生器は、請求項２乃至４のいずれか１項に記載された物理乱数発生器において、前記遅延回路は複数のＳＦＱ素子を直列接続したジョセフソン伝送線路で構成され、前記ＡＮＤ回路は一つの超電導リングにＳＦＱの通過する２個の入力用と１個の出力用のジョセフソン素子を有するＳＦＱ素子を含む複数のＳＦＱ素子により構成されていることを特徴としている。

【００３０】

ここで、「ＳＦＱ素子」とは、ごく薄い絶縁膜からなるジョセフソン接合を超導電材からなる超導電リングの間に挟んだ構造の１単位の超電導素子である。このＳＦＱ素子により遅延回路及びＡＮＤ回路を構成することで、５０Ｇ／ｓを超えるクロック速度を実現する超高速論理動作が可能になる。

【００３１】

次に、請求項６に記載の物理乱数発生器は、請求項１乃至４のいずれか１項に記載された物理乱数発生器において、前記論理回路が入力部にＡＮＤ回路を有するフリップフロップ回路からなることを特徴としている。

【００３２】

フリップフロップ回路は２つの入力信号のレベルと入力時刻に依存して出力が“０”または“１”に変化する。例えば、フリップフロップ回路としてＤ型フリップフロップを用いる場合は、遅延時間揺らぎを有する遅延回路の出力を第１入力端であるデータ入力端子に入力し、周期パルスを第２入力端であるクロック端子に入力する。クロック入力端への周期パルスの立ち上がりでデータ入力レベルがサンプリングされその後の出力が決まるので、遅延時間の揺らぎによりデータ入力端子への入力レベルが時間的に揺らぐことで、Ｄ型フリップフロップの出力が“０”または“１”に変化する。遅延時間の揺らぎは熱揺らぎに起因しているので、Ｄ型フリップフロップの出力として物理乱数を得ることができる。

【発明の効果】
【００３３】
本発明によれば、遅延回路による遅延揺らぎに着目したことで、従来の熱雑音による回路中の電流の振幅変動を用いた比較器型乱数発生器に比べて安定性の高い、制御容易な物理乱数発生器が提供され、デジタル情報社会でのデータの安全性を高めることが出来る他、乱数を用いたモンテカルロ法等のシミュレーションを手軽におこなうことが可能になる。
【図面の簡単な説明】
【００３４】
【図１】本発明の実施の形態に係る物理乱数発生器の構成を示すブロック図である。
【図２】図１の論理回路３の入力と出力の関係を説明する図である。
【図３】ジョセフソン伝送路の説明図である。
【図４】ＳＦＱパルスの様子を示す図である。
【図５】ＳＦＱ素子を用いた物理乱数発生器の等価回路図である。
【図６】半導体プロセスで構成したＳＦＱ素子によるＡＮＤ回路の要部の平面図である。
【図７】半導体プロセス技術を用いたＳＦＱ素子の断面図である。
【図８】ＳＦＱ素子によるＡＮＤ回路の２入力間の遅延時間差と“１”の発生確率の特性を示す図である。
【図９】ＳＦＱパルスの伝搬するジョセフソン接合の数をパラメータにした、ジョセフソン伝送路における遅延時間の時間揺らぎを示す図である。
【図１０】バイアス電流をパラメータにしたジョセフソン接合の数とタイミングジッタ（時間揺らぎ）の関係を示す図である。
【図１１】ＳＦＱ回路による物理乱数発生器の制御電流による“１”の発生確率の変化を示す図である。
【図１２】ジョセフソン接合の数によるグレイゾーン幅の変化を示す図である。
【図１３】２個のジョセフソン接合の遅延時間と制御電圧の関係を示す図である。
【図１４】シミュレーションで用いた入力信号とシミュレーション結果の出力信号である。（Ａ）入力のクロック信号である。（Ｂ）出力の乱数である。
【図１５】バイアス電流をパラメータにした乱数発生速度と自己相関関数値の関係を示す図である。
【図１６】ジョセフソン接合の臨界電流密度が１０ＫＡ／ｃｍ^{2}での乱数発生速度と自己相関関数の関係を示す図である。
【図１７】乱数発生器の面積と乱数発生速度の関係を示す図である。
【図１８】比較器型物理乱数発生器の等価回路図である。
【図１９】図１８の比較器型物理乱数発生器の制御電流と“１”出力の発生確率の関係を示す図である。
【図２０】（Ａ）Ｄ型フリップフロップを用いた物理乱数発生器の構成を示すブロック図である。（Ｂ）Ｄ型フリップフロップの内部構成図である。
【発明を実施するための形態】
【００３５】
先ず、図１に示す本発明に係る物理乱数発生器の全体構成を用いて本発明の概要を説明する。図１に示すように、本発明に係る物理乱数発生器は、入力端子Ｉｎと、この入力端子Ｉｎに接続され、且つ複数個の遅延素子４を直列接続した第１及び第２の遅延回路１、２と、第１及び第２の遅延回路１、２の出力端に入力端がそれぞれ接続されたＡＮＤ回路５及び出力回路６を含む論理回路３と、出力端子Ｏｕｔとで構成されている。
【００３６】
ここでは、第１及び第２の遅延回路１、２のうち、一方の遅延回路、例えば第１の遅延回路１は、動作時に遅延時間を制御（以下、可変ともいう）することが可能な遅延回路（以下、可変遅延回路ともいう）とされ、他方の遅延回路、例えば第２の遅延回路２は、遅延時間が固定される遅延回路（以下、固定遅延回路ともいう）とされている。

【００３７】
この物理乱数発生器では、入力端子Ｉｎから第１及び第２の遅延回路１、２に入力パルス、例えば周期パルスが入力され、それぞれ遅延された後、第１及び第２の遅延回路１、２から周期パルスＡ，Ｂがそれぞれ出力される。この第１及び第２の遅延回路１、２からの周期パルスＡ，ＢはＡＮＤ回路５に入力され、２つの周期パルスＡ，ＢがＡＮＤ回路５の反応するパルス幅（反応時間差Ｔｈ）の中に存在すれば、図２に示すようにＡＮＤ回路５での遅延後に、出力回路６を介して出力端子Ｏｕｔに１レベルの信号が確率５０％以上で発生する。
【００３８】
第１及び第２の遅延回路１、２の遅延時間は、熱による時間揺らぎを有する。そのため、遅延回路１、２から出力される周期パルスは、時間揺らぎを受けて、本来のパルス周期により決まるタイミング時間を中心にして前後した時刻にＡＮＤ回路５へ入力される。
【００３９】
図２にＡＮＤ回路５の２つの入力信号Ａ、Ｂの様子とその信号相互の時間関係による出力信号の様子を示す。ＡＮＤ回路５に入力されるパルスの相対的な時間差が反応時間差Ｔｈよりも小さければ、ＡＮＤ回路５の出力は“１”となり、逆に相対的な時間差が反応時間差Ｔｈよりも大きければ、ＡＮＤ回路５の出力は“０”となる確率が高い。図２において、信号Ａと信号Ｂとの対応するパルスの時間差であるＴｄ１とＴｄ３は反応時間差Ｔｈよりも小さく、Ｔｄ２とＴｄ４は反応時間差Ｔｈよりも大きい場合を示している。
【００４０】
ここで、遅延回路１、２の遅延時間の設定について説明する。遅延回路１、２を長くして遅延時間を増やしていくと遅延時間の時間揺らぎが大きくなる。遅延時間と遅延の時間揺らぎの関係は予め求めることができる。
【００４１】
遅延回路１、２での遅延時間揺らぎの分布は、通常は、平均値を中心にして進み時間と遅れ時間とほぼ同等になる。またＡＮＤ回路５は、２つの入力される周期パルス（以下、周期パルス入力ともいう）の時間差が有る幅（反応時間差Ｔｈ）内であれば、出力に“１”を発生する確率が高くなり、反応時間差Ｔｈを超えると“０”を発生する確率が高くなる。
【００４２】
そこで、先ず周期パルス入力に対するＡＮＤ回路５の反応時間差Ｔｈを求め、次に第１及び第２の遅延回路１、２の遅延時間を変えたときの遅延時間揺らぎの時間分布を求めて、その時間分布において反応時間差Ｔｈよりも大きい部分の面積と小さい部分の面積の割合を所定の大きさになるように遅延時間を選定することで所定の確率でＡＮＤ回路５の出力の“０”と“１”の発生確率を設定することができる。
【００４３】
ＡＮＤ回路５への２つの周期パルス入力の相対的な時間差を反応時間差Ｔｈよりも大きくするとＡＮＤ回路５の出力で“１”を発生する確率は５０％よりも小さくなるが、遅延時間揺らぎがあると、２つの周期パルスの重なり方向への時間揺らぎにより、“１”を発生する確率が高くなる。
【００４４】
逆に２つの周期パルス入力の時間差を反応時間差Ｔｈよりも小さくすると、“１”を発生する確率は５０％よりも大きくなるが、遅延時間揺らぎがあると、２つの周期パルスの離れ方向への時間揺らぎにより、ＡＮＤ回路５の出力で“１”を発生する確率が小さくなる。
【００４５】
つまり、２つの周期パルス入力の相対的な時間差による“１”の発生確率の変化の様子が遅延時間揺らぎにより緩和される。すなわち、遅延時間の時間揺らぎが大きくなると、２つの周期パルス入力の時間差の変化に対して、出力の“１”の発生確率の変化の様子が緩やかになる。つまり、グレイゾーン幅がひろがるので、遅延時間の時間揺らぎを有する

遅延回路１の出力をＡＮＤ回路５へ入力して基準となる時刻と比較する際の、“１”の発生確率５０％を与える２つの周期パルス入力の時間差の設定が容易になる。

【００４６】

次に、遅延時間差に伴う“１”の発生確率が滑らかであれば、ＡＮＤ回路５の第１の入力と第２の入力での周期パルスの平均遅延時間における時間差がパルス周期の自然数倍に前記の反応時間差Ｔｈを加減した値となるように設定する。また、遅延時間差に伴う“１”の発生確率が滑らかでない場合は、動作時に“１”の発生確率が５０％になるように遅延時間差を選ぶ。こうすることで、ＡＮＤ回路５へ周期的に入力される周期パルスの遅延時間の自然な揺らぎに伴いＡＮＤ回路５からは“０”または“１”の信号がランダムに出力される。

【００４７】

また、第１及び第２の遅延回路１、２のうち、少なくとも一方を可変遅延回路とすることで、動作時に遅延時間を調整して、ＡＮＤ回路５の出力における“０”と“１”の発生確率を同じにして一様乱数を得ることもできる。遅延時間を可変（制御）にするには、例えば遅延回路１への供給電圧を変えることで容易に行うことができる。遅延時間の制御は、遅延回路の一つを可変遅延回路にする場合に限らず、２つの遅延回路１、２を共に可変にしても良く、また、一つの遅延回路、例えば第２の遅延回路２を省略して入力端子Ｉｎからの周期パルスを直接、ＡＮＤ回路５の第２入力端へ入力するようにしてもよい。

【００４８】

ここで、周期パルスのパルス波形によっても“１”の発生確率が変化するが、パルスの立ち上がり、立下りの時間が大きい場合は、多少の時間揺らぎがあっても“１”の発生確率への影響が少なくなるので好ましくない。具体的には、周期パルスのパルス幅を反応時間差Ｔｈ以内に狭くすることで、高感度での時間揺らぎの影響を検出することができる。

【００４９】

次に、第１の実施例として、ＳＦＱ素子により構成した物理乱数発生器を説明する。図１に示す第１の遅延回路１及び第２の遅延回路２を、遅延素子４としてＳＦＱ素子を用いたジョセフソン伝送路２０、３０で構成する。このジョセフソン伝送路２０、３０は図３に示すように、複数個のＳＦＱ素子２１、３１を直列接続することにより構成され、各ＳＦＱ素子２１、３１には、バイアス回路（図示略）からＤＣバイアス電流が供給される。各ＳＦＱ素子２１、３１は、超電導リングＲの一部にジョセフソン接合Ｊａ，Ｊｂを有する。このＳＦＱ素子２１、３１に外部から微小な磁界を加えると、超電導リングＲの中には単一の量子化された磁束（ＳＦＱ）が進入する。

【００５０】

このＳＦＱ素子２１、３１を構成する超電導リングＲの中では、磁束は2.07×10^{-15}Ｗｂを単位に量子化された単一磁束量子（ＳＦＱ）となる。ＳＦＱ素子２１、３１は、超電導リングＲに含まれるジョセフソン接合Ｊａ，Ｊｂを常電導化することでスイッチさせることにより、ＳＦＱの超電導リングＲへの出入りを制御する。ＳＦＱ素子２１、３１のスイッチングスピードは、半導体素子の約１００倍、消費電力は約１／１０００である。

【００５１】

そして、このジョセフソン伝送路２０にＤＣバイアス電流（図中で上方から下方に向かう矢印で示している）を流し、例えば、入力端子側のＳＦＱ素子２１、３１の超電導リングＲに微小な磁場を加えると、超電導リングＲにＳＦＱが進入する。

【００５２】

ＳＦＱが進入した超電導リングＲには、ＳＦＱによる電流とバイアス電流が合わさった電流が流れる。図３のように、ＳＦＱを紙面の手前から背面方向へ取り込むと、ＳＦＱの存在する超導電リングＲでは、バイアス電流に加えてジョセフソン接合Ｊｂと隣のＳＦＱ素子２１、３１のジョセフソン接合Ｊｂ／ＪａにＳＦＱによる電流が加わる。この電流が臨界電流値を超えるとジョセフソン接合Ｊｂと隣のＪａは、常電導となりＳＦＱは右のＳＦＱ素子２１、３１の超電導リングＲへ移動する。

【００５３】
このＳＦＱの移動に要する時間は、２～３ピコ秒と極めて短い時間であり、動作温度４．２Ｋで０．１ピコ秒程度の時間揺らぎを有する。ＳＦＱが超電導リングＲを通過すると、図４に示すような電圧パルス（ＳＦＱパルス）が発生する。
【００５４】
このジョセフソン伝送路２１、３１からなる第１及び第２の遅延回路２０、３０は、図５に示すような等価回路で示される。図中のＬＡ１～ＬＡ５、ＬＢ１～ＬＢ５は、それぞれ超導電リングＲ部分のインダクタンスを表す。また、ＪＡ１～ＪＡ４、ＪＢ１～ＪＢ４は、それぞれジョセフソン接合を表す。
【００５５】
ＡＮＤ回路は、ＳＦＱ素子を用いて、図５に示すように、第１の遅延回路２０の出力に接続された第１の伝送路５１と、第２の遅延回路３０の出力に接続された第２の伝送路５２と、第３の伝送路５３と、ＡＮＤ回路の要部５４とで構成される。
【００５６】
第１、第２及び第３の伝送路５１、５２、５３は、いずれも図３に示すような、複数個のＳＦＱ素子２１（３１）を直列接続することにより構成される。この第１の伝送路５１は、図５の等価回路に示すように、ＳＦＱ素子２１（３１）の超電導リングＲ部分によるインダクタンスＬ１、Ｌ３、Ｌ５，Ｌ７とジョセフソン接合Ｊ１、Ｊ３とで、また第２の伝送路５２は、インダクタンスＬ２、Ｌ４，Ｌ６、Ｌ８とジョセフソン接合Ｊ２、Ｊ４とで、また第３の伝送路５３は、インダクタンスＬ１２、Ｌ１３とジョセフソン接合Ｊ８とで構成される。
【００５７】
また、ＡＮＤ回路の要部５４は、Ｌ９，Ｌ１０，Ｌ１１からなる超電導リングに入力用のジョセフソン接合Ｊ５，Ｊ６と出力用のジョセフソン素子Ｊ７からなる。第１及び第２の伝送路５１，５２からのＳＦＱパルスが反応時間差以内にＡＮＤ回路の要部へ到達すると“１”として発生確率５０％以上でジョセフソン接合Ｊ７を通ってＳＦＱパルスが第３の伝送路５３へ出力される。
【００５８】
図６に、第１、第２及び第３の伝送路５１、５２、５３が接続される結合部分の半導体プロセス技術で作製されたＡＮＤ回路の要部５４の平面図を示す。図５に示す等価回路でのＬ９，Ｌ１０，Ｌ１１は超電導金属の回路パターンで実現される。また、ジョセフソン素子Ｊ５，Ｊ６，Ｊ７は基板に垂直方向でグランドの超電導金属と絶縁薄膜を介するようにして実現される。
【００５９】
そして、第１の伝送路５１のジョセフソン接合Ｊ５と第２の伝送路５２のジョセフソン接合Ｊ６からの出力信号は、それぞれインダクタンスＬ９とＬ１０を通して第３の伝送路５３のインダクタンスＬ１１で合算されて、その合算値が所定の値を超えるとＳＦＱがＪ７とＪ８を通って出力される。
【００６０】
また図７に半導体プロセス技術を用いて構成したＳＦＱ素子の断面図を示す。図７において、点線で囲まれた部分がＳＦＱ素子であり、図中の点線の丸で囲まれた部分に示す、ごく薄い絶縁膜を介して超電導金属が向かい合っている部分がジョセフソン接合である。図中ＣＯＵ及びＢＡＳは超電導金属、例えばニオブで、この部分が図３の超電導リングＲに相当する。
【００６１】
すなわち、ＳＦＱ回路により、図２に示すＡＮＤ回路５の第１及び第２の入力端Ａ、Ｂに、第１及び第２の遅延回路からの出力パルスが所定の時間差内に入力された場合に、出力端子ＯｕｔにＡＮＤ回路５中での遅延時間後、“１”が出力される態様が実現される。
【００６２】
図８にＳＦＱ素子によるＡＮＤ回路における２入力の時間差に対する出力特性を示す。

図８に示すように、このＡＮＤ回路は、２入力の時間差（ΔＴ）が約１．５ｐｓ以内では出力に“１”が生じ、約３．５ｐｓ以上では出力に“０”を生じる。絶対値で１．５から３．５の間は“０”と“１”のどちらが出力されるか明確でないのでグレイゾーンになる。この図で“１”出力の発生確率を５０％にするように２入力の時間差（ΔＴ）が反応時間差Ｔｈになるようにすると、一様乱数を得ることができる。ここで、ＴｈｒとＴｈｆに書き分けているのは、２つの入力の先後により多少値が異なるためである。これは主に使用するパルスの波形に依存している。

【００６３】

２入力の時間差（ΔＴ）をＴｈｒまたはＴｈｆに合わせるには、制御電流（以下、制御電圧ともいう）を第１及び第２の遅延回路１、２のバイアス電流に重畳するか、もしくはバイアス電流と独立して供給することで、第１及び第２の遅延回路１、２の遅延時間の平均値の差を制御する。

【００６４】

次に、図９を用いて、第１及び第２の遅延回路１、２を構成するジョセフソン伝送路２０、３０のタイミングジッタについて説明する。ジョセフソン伝送路２０、３０を伝搬するＳＦＱの伝搬時間は、４．２Ｋの動作時に熱雑音の影響を受けて１ジョセフソン接合あたり０．１ｐｓ程度のタイミングジッタを有する。

【００６５】

したがって、ジョセフソン伝送路２０、３０では、ＳＦＱが通過するジョセフソン接合の数に依存してタイミングジッタが増える。図９に示すように、１０接合（ａ）、５０接合（ｂ）、１００接合（ｃ）の遅延時間の平均値との差を見ると、通過する接合数が増えると遅延時間の平均値からのばらつきが大きくなることが分かる。このばらつきがタイミングジッタである。ＡＮＤ回路へ２つの時間差の有る周期パルスを入力して“１”が生じる確率が５０％となる、ＡＮＤ回路の反応時間差（反応時間差Ｔｈ）を図９の横軸の０の両脇に記す。

【００６６】

ＡＮＤ回路５に入力される遅延時間揺らぎによる信号の到着時間の差が、絶対値で反応時間差Ｔｈよりも大きい場合は、ＡＮＤ回路５の出力が“０”となる確率が高くなる。また、絶対値で反応時間差Ｔｈよりも小さい場合は、ＡＮＤ回路５の出力が１”となる確率が高くなる。したがって、図９において“０”出力と“１”出力の面積の割合が所定の値になるように、第１及び第２の遅延回路１、２におけるジョセフソン伝送路２０、３０のジョセフソン接合の数の差を選べばよいことが分かる。

【００６７】

このタイミングジッタについて、図１０に示すように、バイアス電流をパラメータにしたジョセフソン接合の数に伴う平均的なタイミングジッタの変化の様子が報告（Ｈｉｄｅａｋｉ Ｔｅｒａｉ 他、Ａｐｐｌｉｅｄ Ｐｈｙｓｉｃｓ Ｌｅｔｔｅｒｓ Ｖ．８４，Ｎｏ．１２，ＰＰ２１３３－２１３５， ２２ Ｍａｒｃｈ ２００４）されている。

【００６８】

図１０から分かるように、タイミングジッタは、ジョセフソン伝送路２０、３０を構成するジョセフソン接合の数が増えると、ＳＦＱの通過する超電導リングの数の０．５乗に比例し増加する。また、このタイミングジッタは、バイアス電流が増えると減る傾向がある。つまり、タイミングジッタは、ＳＦＱの伝播するジョセフソン接合の数とバイアス電流に依存する。そして、タイミングジッタが増えるとＡＮＤ回路５の二つの入力の時刻差による“１”の発生確率の変化の様子が緩やかになり、グレイゾーン幅が広がることになる。

【００６９】

次に、グレイゾーン幅とジョセフソン素子の数の関係について説明する。図１１にジョセフソン伝送路へ流入する電流と電流の変化による遅延時間の変化による“１”の発生確率の変化の様子を示す。○が実測値であり実線はフィッティングしたものである。この図からグレイゾーン幅は約４０μＡあることが分かる。流入電流と“１”の発生確率の特性

は、前（フロント）側の“１”の立ち上がり部分と後ろ（リア）側の立下り部分があり若干特性が異なるのでグレイゾーン幅の広い方を使用することが好ましい。

【００７０】

図１２にジョセフソン接合の数の変化に伴うグレイゾーン幅の変化の様子を示す。○が前側、□が後ろ側での特性である。共に、ジョセフソン接合の数が増えるとグレイゾーン幅が増えることが分かる。実測値にフィッティングさせた特性は共に、グレイゾーン幅がジョセフソン接合の数の平方に比例していることが分かる。これから、グレイゾーン幅を増やして制御時の安定性を増すには、所定の安定性を得られるようにジョセフソン接合の数を増やせば良いことが分かる。

【００７１】

上記により、遅延回路を構成する遅延素子の数については、グレイゾーン幅を増やすには多くの遅延素子を使い、“１”の発生確率を５０％になるように２つの遅延回路の遅延時間の差を与えるような遅延素子の数の差を持たせればよいことが分かる。

【００７２】

ＳＦＱ回路の特性、４．２Ｋにおけるタイミングジッターを加味したシミュレーションを図１４（Ａ）に示す入力を用いて、クロック周波数１０ＧＨｚで行い、図１４（Ｂ）示す物理乱数を得た。

【００７３】

ところで、実回路で２進乱数の“１”の発生確率を正確に５０％にするには、図８に示す出力での“１”の発生確率が５０％になる反応時間差Ｔｈを目指すように、第１及び第２の遅延回路１、２の遅延時間差を精密に調整する必要がある。

【００７４】

そこで、ジョセフソン伝送路２０、３０の遅延時間がバイアス電流に依存していることに着目した。図１３に示すように、制御電圧により遅延時間が変化する。この遅延時間の変化は２個のジョセフソン接合の臨界電流密度が２．５ＫＡ／ｃｍ^{2}及び１０ＫＡ／ｃｍ^{2}の回路を用いた場合に実験的に得たものである。この図から０．１ピコ秒オーダーでの遅延時間の変化が起こせることが分かる。

【００７５】

この制御電圧による出力の“１”の発生確率を正確に５０％にする制御特性の傾斜が急峻な場合は外乱により制御電流の僅かな変化で出力の“１”の発生確率が大幅に変化することになる。

【００７６】

上記した本実施例の物理乱数発生器によれば、以下のような効果が得られる。先に本願発明者が開発。報告した図１８の比較器型物理乱数発生器では、ＳＦＱ比較器出力の“１”の発生確率が５０％となる動作点は、図１９に示すようなグレイゾーン幅が狭い制御特性を有していた。実験装置では４９．１μＡに設定し実用的な制御電流の許容変化幅は０．７μＡだった。つまり、０．７／４９．１＝１．４％に制御する必要がある。この物理乱数発生器を稼働させて出力測定をすると外部電源電圧の変動の影響を受けて１レベルの発生確率が大きく変動した。図１９において○は熱雑音を考慮したシミュレーション結果、□は熱雑音が無い場合のシミュレーション結果である。熱雑音の存在によりグレーゾーン幅が拡大することが分かる。

【００７７】

これに対して、本実施例による物理乱数発生器では、ＳＦＱ素子によるＡＮＤ回路を使い、熱雑音を直接用いることなく熱雑音の影響を受けて伝搬遅延時間が揺らぐ現象を用いる。そのため、グレイゾーン幅が広くなり外部電圧の変動があっても、“１”の５０％の発生確率を安定に維持することができる。

【００７８】

具体的には、図８に示される入出力特性を有するＡＮＤ回路において“１”の発生確率５０％を目的とするＴｈの時間の設定精度（Δｔ）として０．５ｐｓとすると、図１３において１０ＫＡ／ｃｍ^{2}では制御電圧に対する遅延時間の変化率は１．５ｐｓ／ｍｖの特

性なのでΔｔ＝０．５ｐｓを制御するにはΔＶ＝０．３３ｍｖを制御する必要がある。中心電圧２．５ｍｖに対して０．３３ｍｖは１３％であり、従来例のＳＦＱ比較器を用いた物理乱数発生器の制御の要求精度の１．４％に比べ一桁制御の安定度が向上することが分かる。

【００７９】

図１５に本実施例の物理乱数発生器における乱数の自己相関特性を示す。この図から本実施例の物理乱数発生器によれば、６０Ｇｂｉｔ／ｓを達成することができることが分かる。また、図１６に本実施例の物理乱数発生器におけるバイアス電流１０ＫＡ／ｃｍ^{2}での乱数発生速度と隣り合うビットとの自己相関関数の特性を示す。相関関数は無相関を示す０が理想である。本実施例の物理乱数発生器では、相関関数は６０Ｇｂｉｔ／ｓを超えると特性が段々劣化するが、６０Ｇｂｉｔ／ｓまでは、相関関数がほぼ０の乱数が得られることが分かる。

【００８０】

物理乱数発生器は半導体プロセス技術で作製されるので、図１７に占有面積と速度による本実施例の物理乱数発生器の位置づけを示す。本実施例の物理乱数発生器は、従来の半導体回路を用いた乱数発生器と同様の占有面積で、従来より遥かに高速での物理乱数の発生が可能である。

【００８１】

次に、第２の実施例として、通常の半導体回路により構成した物理乱数発生器について、図２０を用いて説明する。図２０（Ａ）に示しように、この実施例の物理乱数発生器では、遅延回路７０及び論理回路８０は、Ｄ型フリップフロップＤ－ＦＦで構成される。遅延回路７０は、複数個の遅延素子４としてのＤ型フリップフロップＤ－ＦＦを直列接続してなり、遅延回路７０には入力端子Ｉｎから周期パルスが入力される。論理回路８０のＤ型フリップフロップＤ－ＦＦのＤ端子には遅延回路７０からの出力が入力され、クロック端子ＣＬＫには入力端子からの周期パルスが直接入力される。

【００８２】

Ｄ型フリップフロップＤ－ＦＦは、図２０（Ｂ）に示すように、ＡＮＤ回路にインバータを付加したＮＡＮＤ回路の組み合わせにより構成される。つまり、Ｄ型フリップフロップＤ－ＦＦを用いる場合も、２つの信号の入力時間差の重なり具合を調べる回路はＡＮＤ回路となる。

【００８３】

上記構成の第２の実施例による物理乱数発生器においても、遅延回路による遅延時間揺らぎを用いることで、１レベル信号の発生確率特性の傾斜が緩やか（「傾きが小さい」ともいう）で、グレイゾーン幅を広くできる。また、遅延時間を増やすことでグレイゾーン幅を増やすことができる。したがって、上記第１の実施例と同様、外部電圧の変動に対して動作が安定になる。

【産業上の利用可能性】

【００８４】

本発明は従来の電流または電圧の振幅方向での揺らぎでなく時間方向での揺らぎに基づいて物理乱数を発生するので、調整が容易で安定な物理乱数発生器を実現できる。特にＳＦＱ素子を用いることで省電力、高速性の両立を図ることが可能になった。物理乱数はこれからの情報がデジタル化される社会で必須の要素技術でありその社会的な効用は大きい。

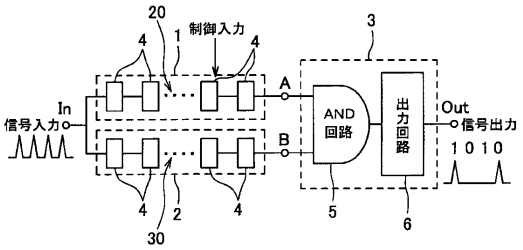
【符号の説明】

【００８５】

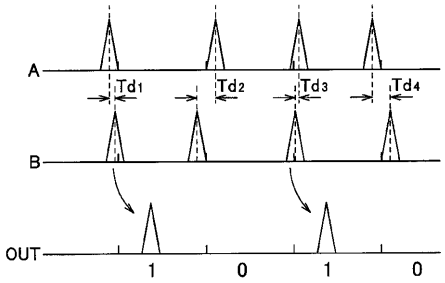
１　第１の遅延回路
２　第２の遅延回路
３　論理回路
４　遅延素子
５　ＡＮＤ回路

６　出力回路
Ｒ　超電導リング
Ｊａ、Ｊｂ　ジョセフソン接合
２０、３０　ジョセフソン伝送路
２１、３１　ＳＦＱ素子
５１　第１の伝送路
５２　第２の伝送路
５３　第３の伝送路
５４　ＡＮＤ回路の要部
７０　遅延回路
８０　論理回路

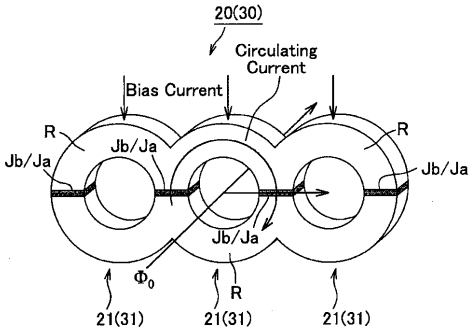
【図１】



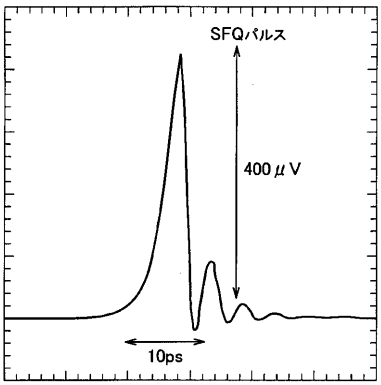
【図２】



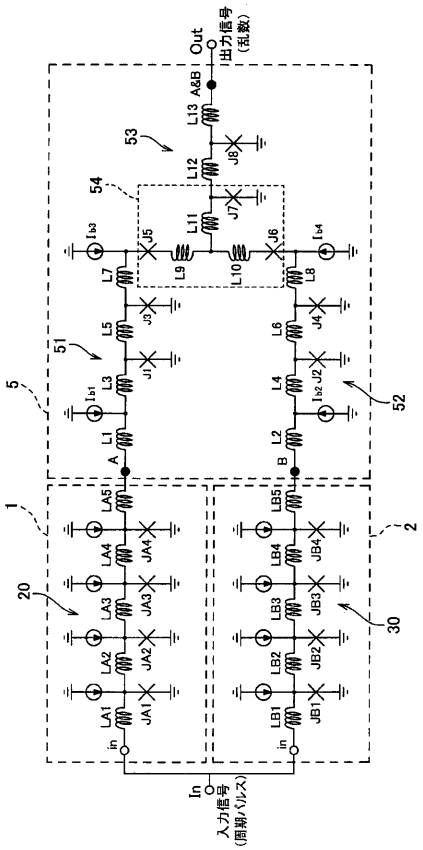
【図３】



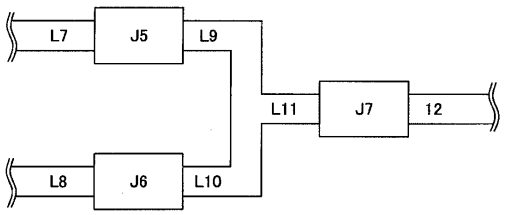
【図４】



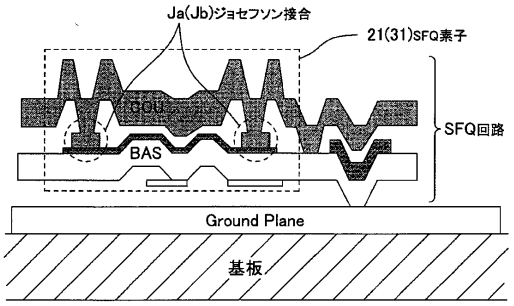
【図５】



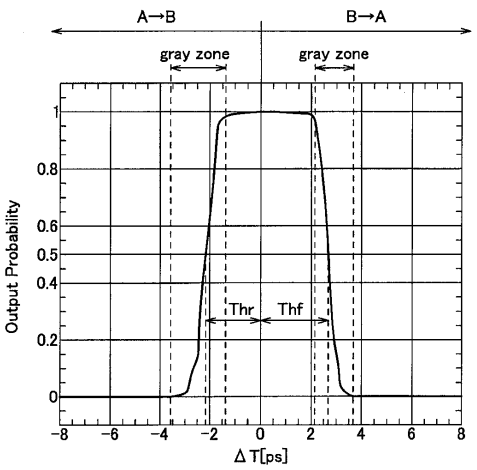
【図６】



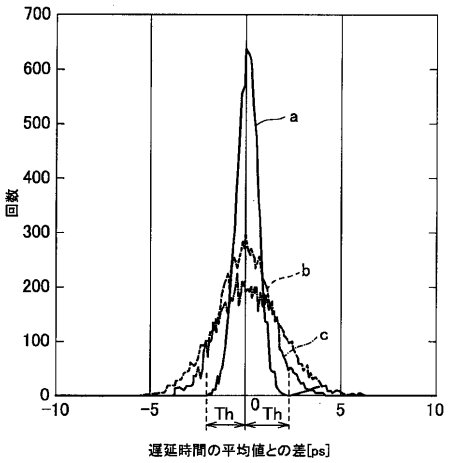
【図７】



【図８】

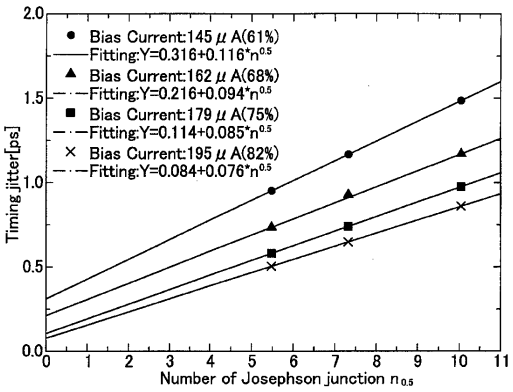


【図９】

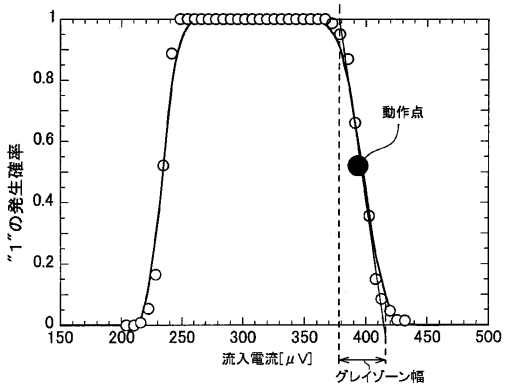


a: 10接合伝播後
b: 50接合伝播後
c: 100接合伝播後

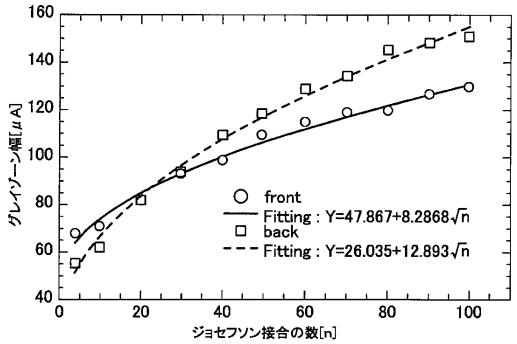
【図１０】



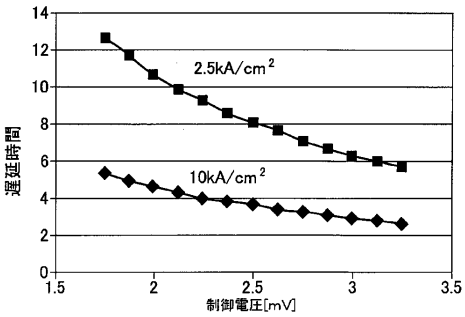
【図１１】



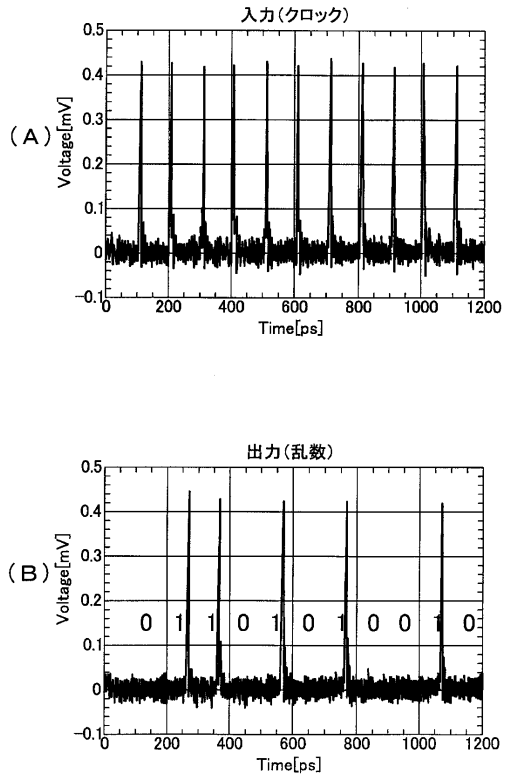
【図１２】



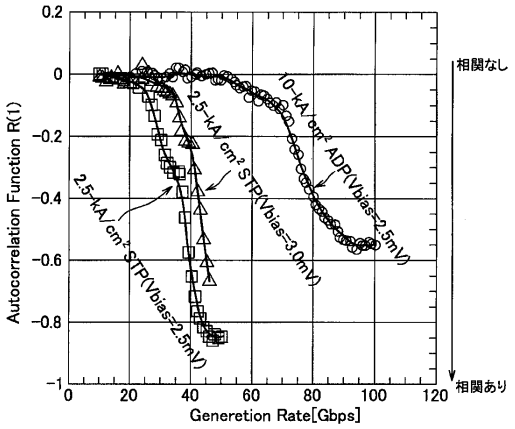
【図１３】



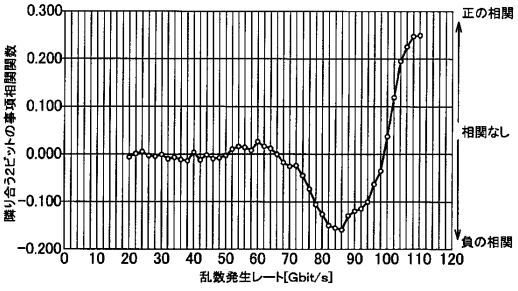
【図１４】



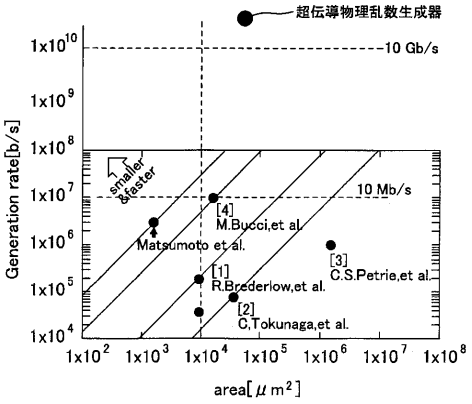
【図１５】



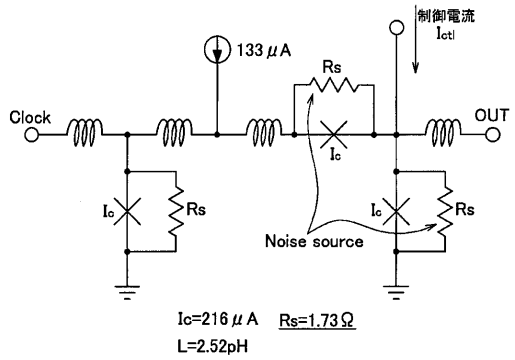
【図１６】



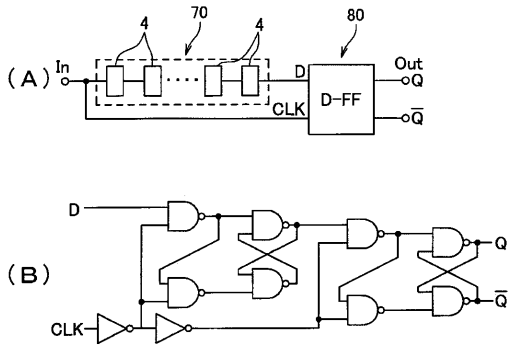
【図１７】



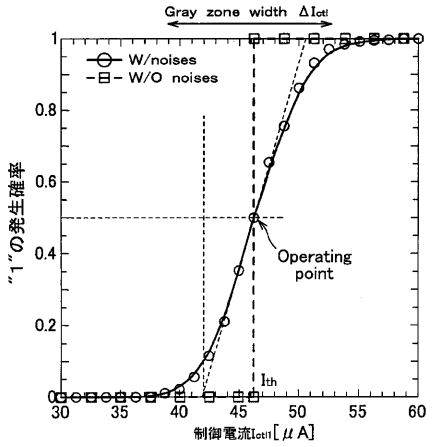
【図１８】



【図２０】



【図１９】



フロントページの続き

(74)代理人 100166110
弁理士 吉田 裕二
(72)発明者 山梨 裕希
神奈川県横浜市保土ヶ谷区常盤台７９番１号 国立大学法人横浜国立大学内
(72)発明者 杉浦 達郎
神奈川県横浜市保土ヶ谷区常盤台７９番１号 国立大学法人横浜国立大学内

審査官 田川 泰宏

(56)参考文献 特開平１０－０５１２７６（ＪＰ，Ａ）
特開２００６－２９４００１（ＪＰ，Ａ）
特開２００１－１３６０５３（ＪＰ，Ａ）
特開２００９－１６３５３９（ＪＰ，Ａ）
福島 章雄，スピンダイス：トンネル磁気抵抗素子を用いた物理乱数発生器，２０１０年 暗号と情報セキュリティシンポジウム ＳＣＩＳ２０１０ 予稿集 ［ＣＤ－ＲＯＭ］，電子情報通信学会情報，２０１０年 1月１９日
Yuki Yamanashi, Superconductive random number generator using thermal noises in SFQ circuits, Applied Superconductivity, IEEE Transactions on, ２００９年 6月, Vol.19,No.3, p.630-633

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ７／５８
Ｇ０９Ｃ １／００
Ｈ０４Ｌ ９／１０