

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2012-220968

(P2012-220968A)

(43) 公開日 平成24年11月12日(2012.11.12)

(51) Int.Cl.			F I	テーマコード (参考)		
<b>G06F</b>	<b>7/58</b>	<b>(2006.01)</b>	G06F 7/58	A	5 J 1 0 4	
<b>G09C</b>	<b>1/00</b>	<b>(2006.01)</b>	G09C 1/00	6 5 0 B		
<b>H04L</b>	<b>9/10</b>	<b>(2006.01)</b>	H04L 9/00	6 2 1 Z		

審査請求 未請求 請求項の数 6 O L (全 18 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)

特許法第30条第1項適用申請有り 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

(71) 出願人 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

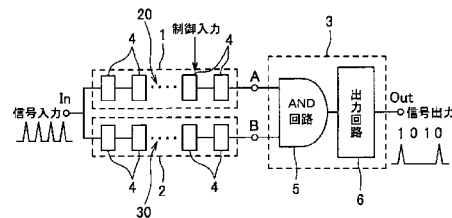
(54) 【発明の名称】 物理乱数発生器

(57) 【要約】

【課題】 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。

【解決手段】 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:  $T_h$ ) のときに確率50%で“1”の信号を出力する。

【選択図】 図1



**【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： $T_h$ ）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。

10

**【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。

20

**【請求項 5】**

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 1 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する請求項 1 乃至 4 いずれか 1 項に記載の物理乱数発生器。

30

**【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。

40

**【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ェ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ェアプログラムで 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。

50

## 【 0 0 0 5 】

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）。

## 【 0 0 0 6 】

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。

10

## 【 0 0 0 7 】

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。

## 【 0 0 0 8 】

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）。

## 【 0 0 0 9 】

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。

20

## 【 0 0 1 0 】

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（ $\Phi_0 = h / 2e = 2.07 \times 10^{-15} \text{ Weber}$ 、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。

## 【 0 0 1 1 】

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 $\Phi_0$ 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 $I_c$ で表すと、 $L \cdot I_c$ が $\Phi_0$ 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、 $L \cdot I_c$ が $\Phi_0$ の0.5倍程度に設計パラメータを定める。

30

## 【 0 0 1 2 】

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（ $\mu W$ ）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。

## 【 0 0 1 3 】

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。

40

## 【 0 0 1 4 】

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 $I_{c1}$ 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

50

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 Physical Random Number Generator Using Thermal Noises in SFQ Circuits」, IEEE Tr. on Applied Superconductivity, Vol. 19, No. 3 June 2009

10

【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。

20

【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。

30

【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。

40

【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

50

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（ $T_h$ ）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 $T_h$ 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

10

20

30

40

50

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。

10

【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。

20

【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。

30

【図2】図1の論理回路3の入力と出力の関係を示す図である。

【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。

40

【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。

50

【図16】ジョセフソン接合の臨界電流密度が  $10 \text{ kA/cm}^2$  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  $I_n$  と、この入力端子  $I_n$  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  $O_{ut}$  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  $I_n$  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  $T_h$ )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  $O_{ut}$  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  $T_h$  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  $T_h$  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  $T_{d1}$  と  $T_{d3}$  は反応時間差  $T_h$  よりも小さく、 $T_{d2}$  と  $T_{d4}$  は反応時間差  $T_h$  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  $T_h$ )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  $T_h$  を超えると“0”を発生する確率が高くなる。

【0042】

10

20

30

40

50

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 $T_h$ 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 $T_h$ 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く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 $T_h$ 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。

10

【0044】

逆に2つの周期パルス入力の時間差を反応時間差 $T_h$ 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。

20

【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 $T_h$ 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。

30

【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 $T_h$ 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。

40

【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 $J_a$ 、 $J_b$ を有す

50



る。この S F Q 素子 2 1、3 1 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 ( S F Q ) が進入する。

【 0 0 5 0 】

この S F Q 素子 2 1、3 1 を構成する超電導リング R の中では、磁束は  $2.07 \times 10^{-15}$  W b を単位に量子化された単一磁束量子 ( S F Q ) となる。S F Q 素子 2 1、3 1 は、超電導リング R に含まれるジョセフソン接合 J a , J b を常電導化することでスイッチさせることにより、S F Q の超電導リング R への出入りを制御する。S F Q 素子 2 1、3 1 のスイッチングスピードは、半導体素子の約 1 0 0 倍、消費電力は約 1 / 1 0 0 0 である。

【 0 0 5 1 】

そして、このジョセフソン伝送路 2 0 に D C 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 S F Q 素子 2 1、3 1 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 S F Q が進入する。

【 0 0 5 2 】

S F Q が進入した超電導リング R には、S F Q 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、S F Q を紙面の手前から背面方向へ取り込むと、S F Q の存在する超電導リング R では、バイアス電流に加えてジョセフソン接合 J b と隣の S F Q 素子 2 1、3 1 のジョセフソン接合 J b / J a に S F Q 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 J b と隣の J a は、常電導となり S F Q は右の S F Q 素子 2 1、3 1 の超電導リング R へ移動する。

【 0 0 5 3 】

この S F Q 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 . 2 K で 0 . 1 ピコ秒程度の時間揺らぎを有する。S F Q 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 ( S F Q パルス ) が発生する。

【 0 0 5 4 】

このジョセフソン伝送路 2 1、3 1 からなる第 1 及び第 2 の遅延回路 2 0、3 0 は、図 5 に示すような等価回路で示される。図中の L A 1 ~ L A 5、L B 1 ~ L B 5 は、それぞれ超電導リング R 部分のインダクタンスを表す。また、J A 1 ~ J A 4、J B 1 ~ J B 4 は、それぞれジョセフソン接合を表す。

【 0 0 5 5 】

A N D 回路は、S F Q 素子を用いて、図 5 に示すように、第 1 の遅延回路 2 0 の出力に接続された第 1 の伝送路 5 1 と、第 2 の遅延回路 3 0 の出力に接続された第 2 の伝送路 5 2 と、第 3 の伝送路 5 3 と、A N D 回路の要部 5 4 とで構成される。

【 0 0 5 6 】

第 1、第 2 及び第 3 の伝送路 5 1、5 2、5 3 は、いずれも図 3 に示すような、複数個の S F Q 素子 2 1 ( 3 1 ) 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 5 1 は、図 5 の等価回路に示すように、S F Q 素子 2 1 ( 3 1 ) の超電導リング R 部分によるインダクタンス L 1、L 3、L 5、L 7 とジョセフソン接合 J 1、J 3 とで、また第 2 の伝送路 5 2 は、インダクタンス L 2、L 4、L 6、L 8 とジョセフソン接合 J 2、J 4 とで、また第 3 の伝送路 5 3 は、インダクタンス L 1 2、L 1 3 とジョセフソン接合 J 8 と

【 0 0 5 7 】

また、A N D 回路の要部 5 4 は、L 9、L 1 0、L 1 1 からなる超電導リングに入力用のジョセフソン接合 J 5、J 6 と出力用のジョセフソン素子 J 7 からなる。第 1 及び第 2 の伝送路 5 1、5 2 からの S F Q パルスが反応時間差以内に A N D 回路の要部へ到達すると“ 1 ”として発生確率 5 0 % 以上でジョセフソン接合 J 7 を通って S F Q パルスが第 3 の伝送路 5 3 へ出力される。

【 0 0 5 8 】

図 6 に、第 1、第 2 及び第 3 の伝送路 5 1、5 2、5 3 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 A N D 回路の要部 5 4 の平面図を示す。図 5 に示す等価回路で

10

20

30

40

50

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ウ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を通して出力される。

【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。

10

【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”が出力される態様を実現される。

【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( $T$ )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( $T$ )が反応時間差 $T_h$ 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、 $T_{hr}$ と $T_{hf}$ 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。

20

【0063】

2入力の時間差( $T$ )を $T_{hr}$ または $T_{hf}$ 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。

30

【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 $T_h$ )を図9の横軸の0の両脇に記す。

40

【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 $T_h$ 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 $T_h$ 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

50

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, PP 2133 - 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  $40 \mu\text{A}$  であることが分かる。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、4.2 K 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 10 GHz 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  $T_h$  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  $2.5 \text{ KA/cm}^2$  及び  $10 \text{ KA/cm}^2$  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

10

20

30

40

50

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 $49.1\ \mu\text{A}$ に設定し実用的な制御電流の許容変化幅は $0.7\ \mu\text{A}$ 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イゾーン幅が拡大することが分かる。

10

【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( $t$ )として $0.5\ \text{ps}$ とすると、図13において $10\ \text{KA}/\text{cm}^2$ では制御電圧に対する遅延時間の変化率は $1.5\ \text{ps}/\text{mv}$ の特性なので  $t = 0.5\ \text{ps}$ を制御するには  $V = 0.33\ \text{mv}$ を制御する必要がある。中心電圧 $2.5\ \text{mv}$ に対して $0.33\ \text{mv}$ 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%に比べ制御の安定度が向上することが分かる。

20

【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、 $60\ \text{Gbit}/\text{s}$ を達成することができる。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 $10\ \text{KA}/\text{cm}^2$ 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 $60\ \text{Gbit}/\text{s}$ を超えると特性が段々劣化するが、 $60\ \text{Gbit}/\text{s}$ 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。

30

【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。

40

【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。

50

## 【 0 0 8 3 】

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 】

## 【 0 0 8 4 】

本発明は従来 of 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S F Q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。

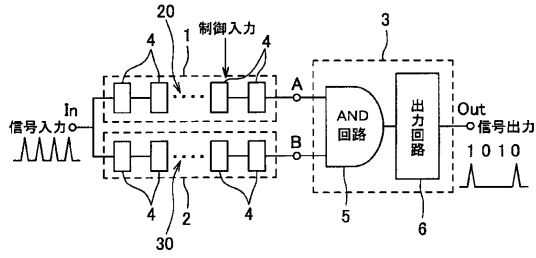
10

## 【 符号の説明 】

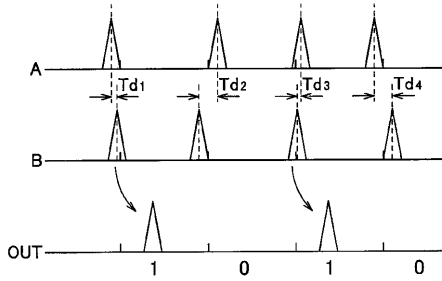
## 【 0 0 8 5 】

- 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 A N D回路 20
- 6 出力回路
- R 超電導リング
- J a、J b ジョセフソン接合
- 2 0、3 0 ジョセフソン伝送路
- 2 1、3 1 S F Q素子
- 5 1 第1の伝送路
- 5 2 第2の伝送路
- 5 3 第3の伝送路
- 5 4 A N D回路の要部
- 7 0 遅延回路 30
- 8 0 論理回路

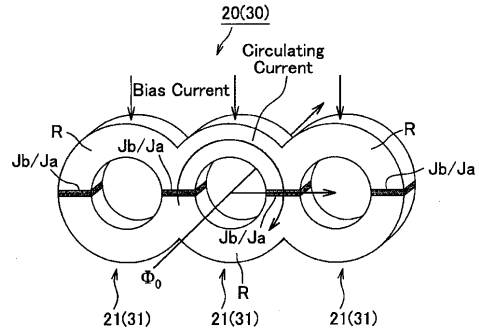
【 図 1 】



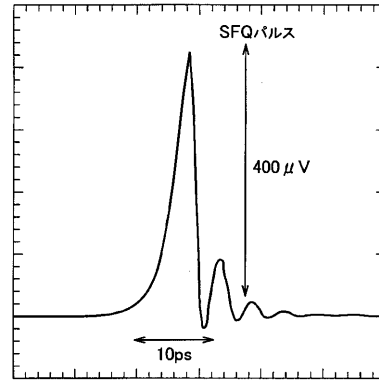
【 図 2 】



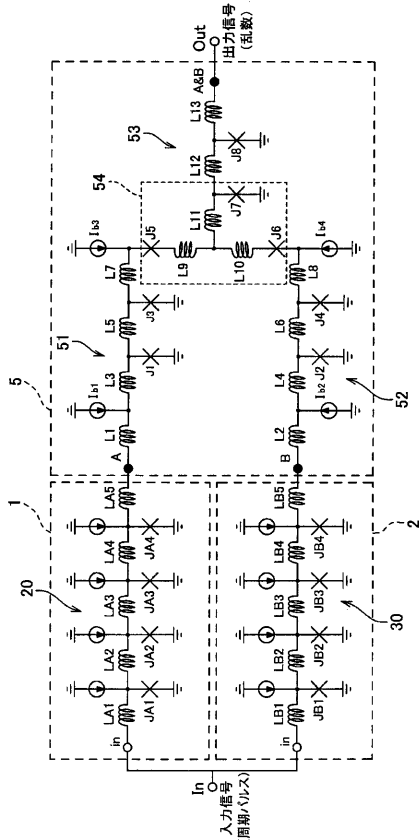
【 図 3 】



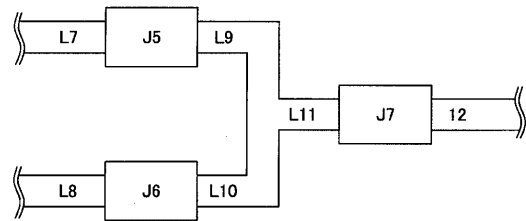
【 図 4 】



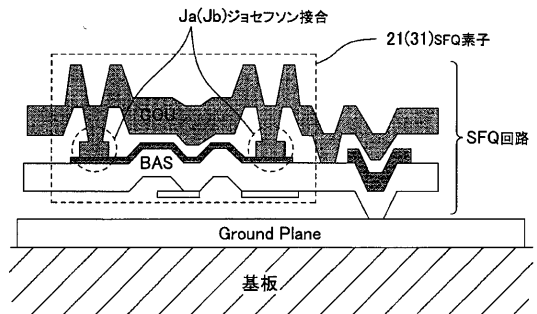
【 図 5 】



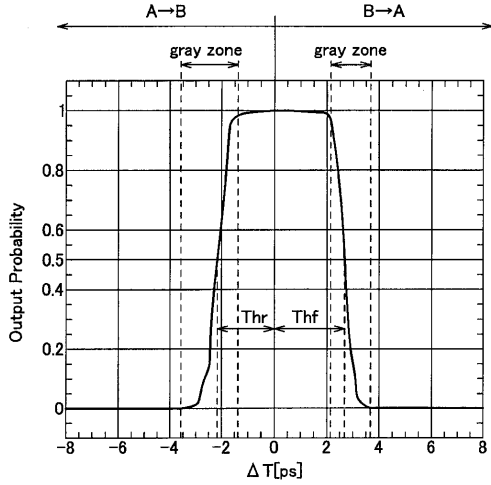
【 図 6 】



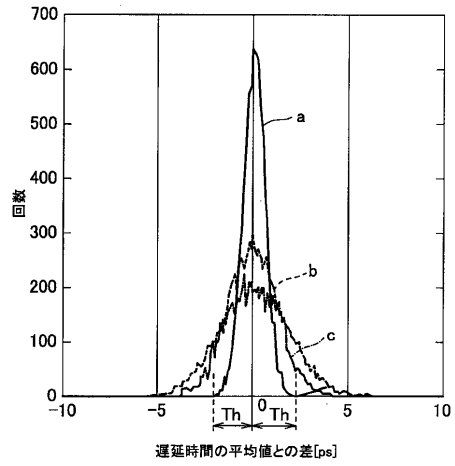
【 図 7 】



【 図 8 】

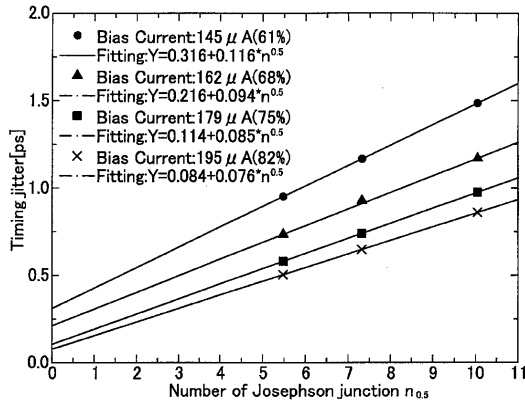


【 図 9 】

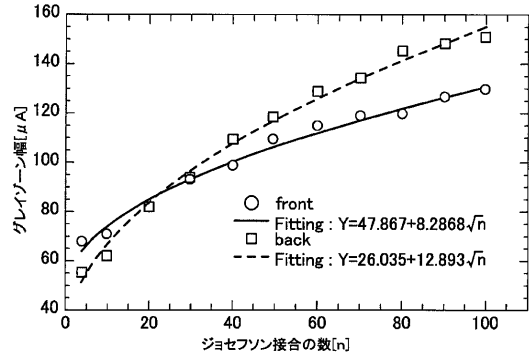


a: 10接合伝播後  
 b: 50接合伝播後  
 c: 100接合伝播後

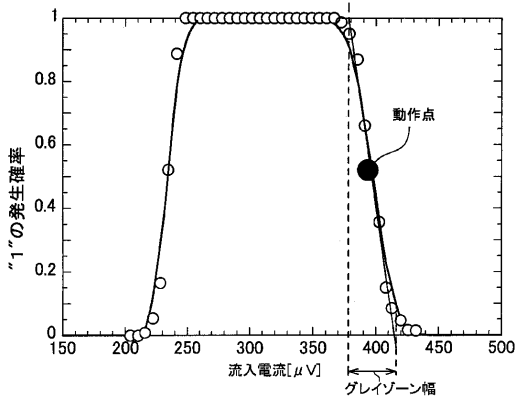
【 図 10 】



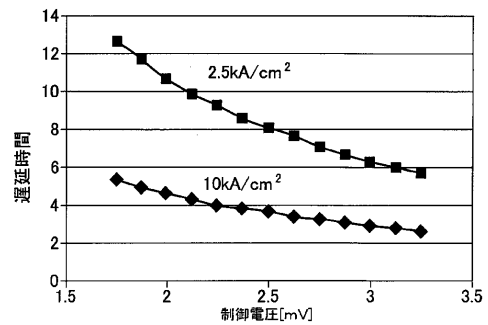
【 図 12 】



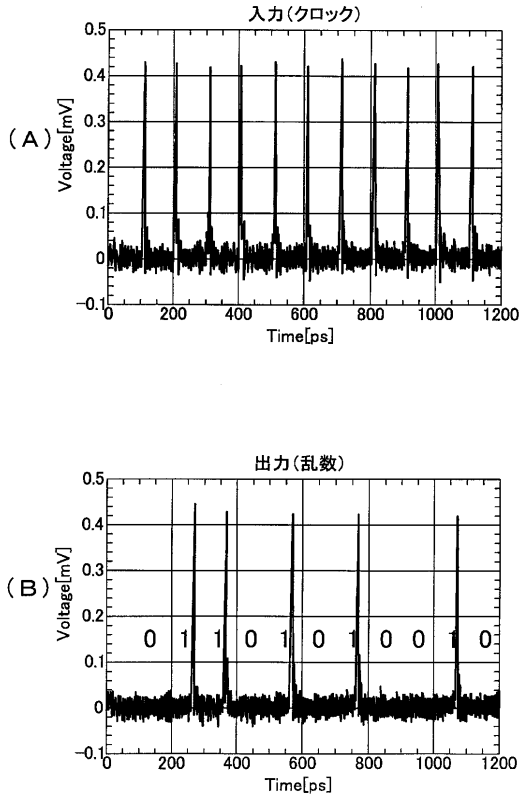
【 図 11 】



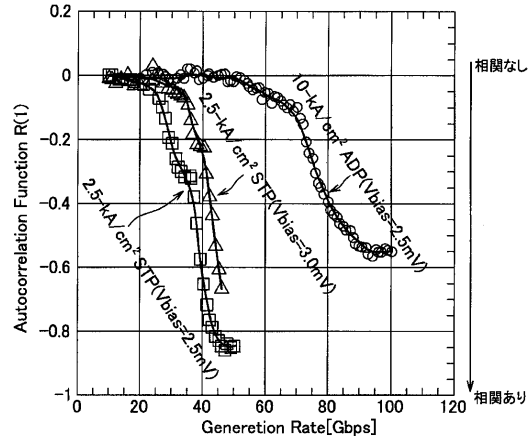
【 図 13 】



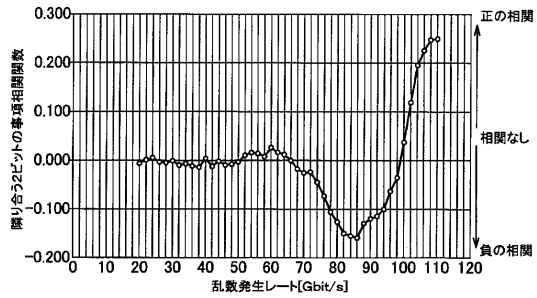
【 図 1 4 】



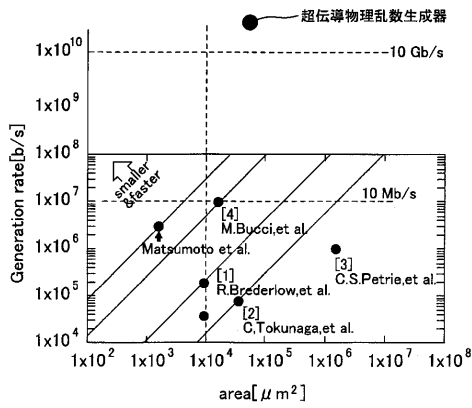
【 図 1 5 】



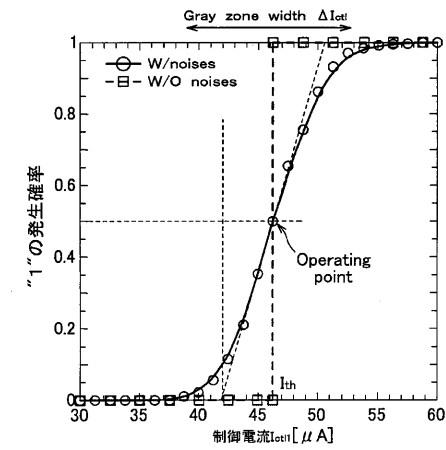
【 図 1 6 】



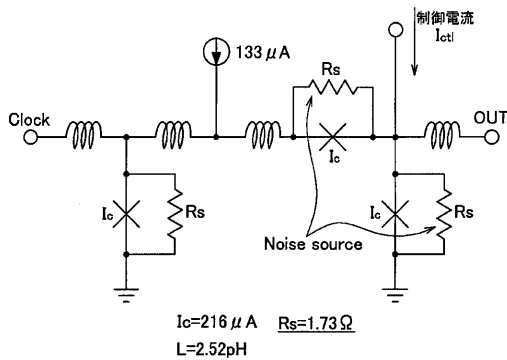
【 図 1 7 】



【 図 1 9 】

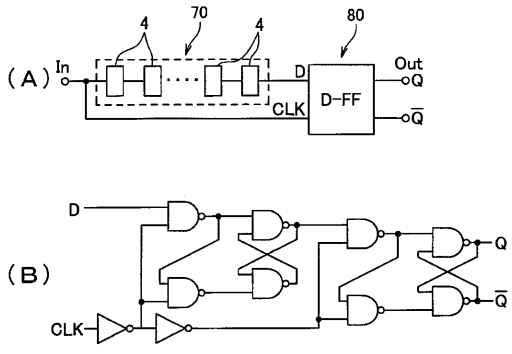


【 図 1 8 】





【 図 2 0 】



---

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7-9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7-9番1号 国立大学法人横浜国立大学内

Fターム(参考) 5J104 FA10 NA42