(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2008-52545
(P2008-52545A)
(43)公開日　平成20年3月6日(2008.3.6)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 7/58	(2006.01)	G06F 7/58	A	

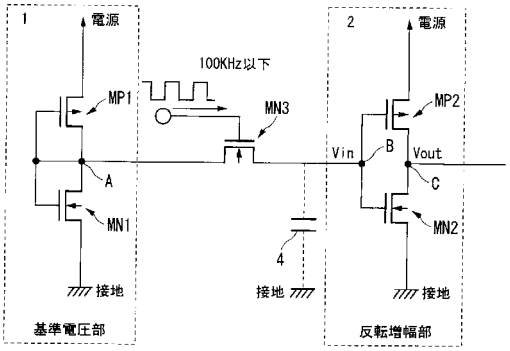
審査請求 未請求　請求項の数 4　ＯＬ　（全 8 頁）

(21)出願番号　特願2006-228975 (P2006-228975)
(22)出願日　平成18年8月25日 (2006.8.25)

(71)出願人　000002325
セイコーインスツル株式会社
千葉県千葉市美浜区中瀬１丁目８番地
(74)代理人　100079212
弁理士　松下　義治
(72)発明者　佐藤　豊
千葉県千葉市美浜区中瀬１丁目８番地　セイコーインスツル株式会社内

(54)【発明の名称】乱数発生回路

(57)【要約】
【課題】　ノイズから物理的乱数を発生させる簡易な回路構成の乱数発生回路を提供する。
【解決手段】　本発明の乱数発生回路は、ソースが電源に接続され、ゲートがドレインに接続された第1Ｐチャネル型ＭＯＳトランジスタと、ソースが接地され、ゲートがドレインに接続され、ドレインが第1Ｐチャネル型ＭＯＳトランジスタのドレインと接続された第1Ｎチャネル型ＭＯＳトランジスタからなる基準電圧部と、ソースが電源に接続された第2のＰチャネル型ＭＯＳトランジスタと、ソースが接地され、ゲートが第2Ｐチャネル型ＭＯＳトランジスタのゲートと接続され、ドレインが第1Ｐチャネル型ＭＯＳトランジスタのドレインと接続された第1のＮチャネル型ＭＯＳトランジスタからなる反転増幅部と、第1Ｐチャネル型ＭＯＳトランジスタのドレインに一端が接続され、第2Ｐチャネル型ＭＯＳトランジスタのゲートに他端が接続された半導体スイッチとを有する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
ソースが電源に接続され、ゲートがドレインに接続された第１のＰチャネルＭＯＳトランジスタと、ソースが接地され、ゲートがドレインに接続され、ドレインが前記第１のＰチャネルＭＯＳトランジスタのドレインと接続された第１のＮチャネルＭＯＳトランジスタとから構成された基準電圧部と、
ソースが電源に接続された第２のＰチャネルＭＯＳトランジスタと、ソースが接地され、ゲートが第２のＰチャネルＭＯＳトランジスタのゲートと接続され、ドレインが前記第１のＰチャネルＭＯＳトランジスタのドレインと接続された第１のＮチャネルＭＯＳトランジスタとから構成された反転増幅部と、
前記第１のＰチャネルＭＯＳトランジスタのドレインに一端が接続され、前記第２のＰチャネルＭＯＳトランジスタのゲートに他端が接続された半導体スイッチと
を有することを特徴とする乱数発生回路。
【請求項２】
前記基準電圧部の基準電圧と、前記反転増幅器の論理閾値電圧とが等しいことを特徴とする請求項１記載の乱数発生回路。
【請求項３】
前記第１のＰチャネルＭＯＳトランジスタと第２のＰチャネルＭＯＳトランジスタとのトランジスタサイズが同一であり、前記第１のＮチャネルＭＯＳトランジスタと第２のＮチャネルＭＯＳトランジスタとのトランジスタサイズが同一であることを特徴とする請求項１または請求項２に記載の乱数発生回路。
【請求項４】
前記半導体スイッチがＭＯＳトランジスタによるトランスファーゲートであることを特徴とする請求項１から請求項３のいずれかに記載の乱数発生回路。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、物理的乱数を発生する乱数発生回路に係わり、例えば、ＩＣカードやプログラム内蔵の１チップマイコンなどのセキュリティ機能に必要な暗号鍵の生成に用いる乱数の発生に適した乱数発生回路に関する。
【背景技術】
【０００２】
ＩＤや暗号キー等の機密保持に用いられる乱数発生回路には高いランダム性が必要とされている。
乱数とは、自然界に存在するランダム現象を利用する物理的乱数と、人為的に作成する疑似乱数に大別される。
ここで、疑似乱数は論理回路やソフトウェアによって、人為的に乱数を生成するものであり、パーソナルコンピュータの組み込み乱数回路等が代表例となっている。
しかしながら、疑似乱数は論理回路やソフトウェアにより乱数発生の手順が決まっているため、システムの初期状態が分ってしまえば、比較的容易に乱数が予測することができ、機密保持が不完全となる場合がある。
【０００３】
一方、一般的に、物理的乱数は、高いランダム特性を持ち、本質的に暗号学的には安全な乱数とみなせる。
例えば、上記物理乱数としては、電気的に抵抗体の熱雑音、半導体のＰＮ接合のショット雑音などがある。
そして、この物理的乱数を用いた乱数発生回路としては、熱雑音素子により発生された熱雑音をサンプリングし、この電荷としてサンプリングして容量手段に蓄え、この容量に蓄積された電圧を増幅し、Ａ／Ｄ変換によりデジタル信号に変換して乱数として出力する技術がある（例えば、特許文献１参照）。

【特許文献１】特開２００１－１７５４５８号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
しかながら、上記物理的乱数は、雑音源からの熱雑音等により生成するが、ノイズレベルが微少（数十～数百μＶ）であり、その熱雑音を有効な乱数として取り出すために高電圧が必要となる。
一方、ＬＳＩの機能の向上による回路の高密度化に対応し、製造における素子微細化が進んでいる。この素子微細化に伴い、素子の耐圧が低下することにより、耐圧が低下してしまう欠点がある。
【０００５】
また、機密保持の観点からは、乱数発生回路をＬＳＩのチップ上に取り込むことが必要となるが、物理的乱数を用いる構成とするため、ＬＳＩ材料としての適合性などの解決すべき課題が多い。
特に、上記従来の乱数発生回路は、ノイズのランダム成分を取り出す手段のノイズ増幅器の具体的な構成における素子数が多く、ＬＳＩチップの面積を増加させてしまう問題があり、製造コストが上昇してしまう問題がある。
本発明は、このような事情に鑑みてなされたもので、物理的乱数の元となるランダム現象のノイズを発生させ、かつこのノイズを検出して乱数を生成する簡易な回路構成の乱数発生回路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】
【０００６】
上述した課題を解決するため、本発明の乱数発生回路は、ソースが電源に接続され、ゲートがドレインに接続された第１のＰチャネルＭＯＳトランジスタと、ソースが接地され、ゲートがドレインに接続され、ドレインが前記第１のＰチャネルＭＯＳトランジスタのドレインと接続された第１のＮチャネルＭＯＳトランジスタとから構成された基準電圧部と、ソースが電源に接続された第２のＰチャネルＭＯＳトランジスタと、ソースが接地され、ゲートが第２のＰチャネルＭＯＳトランジスタのゲートと接続され、ドレインが前記第１のＰチャネルＭＯＳトランジスタのドレインと接続された第１のＮチャネルＭＯＳトランジスタとから構成された反転増幅部と、前記第１のＰチャネルＭＯＳトランジスタのドレインに一端が接続され、前記第２のＰチャネルＭＯＳトランジスタのゲートに他端が接続された半導体スイッチとを有することを特徴とする。
【０００７】
本発明の乱数発生回路は、前記基準電圧部の基準電圧と、前記反転増幅器の論理閾値電圧とが等しいことを特徴とする。
【０００８】
本発明の乱数発生回路は、前記第１のＰチャネルＭＯＳトランジスタと第２のＰチャネルＭＯＳトランジスタとのトランジスタサイズが同一であり、前記第１のＮチャネルＭＯＳトランジスタと第２のＮチャネルＭＯＳトランジスタとのトランジスタサイズが同一であることを特徴とする。
【０００９】
本発明の乱数発生回路は、前記半導体スイッチがＭＯＳトランジスタによるトランスファーゲートであることを特徴とする。
【発明の効果】
【００１０】
以上説明したように、本発明の乱数発生回路によれば、基準電源の発生する微少ノイズを、反転増幅回路にて増幅する構成により、簡易な回路にて物理的乱数を容易に発生させることが可能なため、乱数を生成する回路を構成する素子数を、従来例に比較して削減するこができ、乱数発生の機能を有するＬＳＩのチップサイズを小さくすることとなり、製造コストを減少させることができる。

【発明を実施するための最良の形態】
【００１１】
以下、本発明の一実施形態による乱数発生回路を図面を参照して説明する。図１は同実施形態による乱数発生回路の構成例を示すブロック図である。
この図において、基準電圧部１は、ＰチャネルＭＯＳトランジスタＭＰ１とＮチャネルＭＯＳトランジスタＭＮ１とから構成されている。ＰチャネルＭＯＳトランジスタＭＰ１は、ソースが電源に接続されており、ゲートがドレインに接続されている。ＮチャネルＭＯＳトランジスタＭＮ１は、ソースが接地されており、ゲートがドレインに接続され、かつドレインが上記ＰチャネルＭＯＳトランジスタＭＰ１のドレインに接続されている。
【００１２】
反転増幅部（インバータ）２は、ＰチャネルＭＯＳトランジスタＭＰ２とＮチャネルＭＯＳトランジスタＭＮ２とから構成されている。ＰチャネルＭＯＳトランジスタＭＰ２は、ソースが電源に接続されており、ドレインがＮチャネルＭＯＳトランジスタＭＮ２のドレインに接続されている。ＮチャネルＭＯＳトランジスタＭＮ２は、ソースが接地されており、ゲートが上記ＰチャネルＭＯＳトランジスタのゲートに接続され、かつドレインが上記ＰチャネルＭＯＳトランジスタＭＰ２のドレインに接続されている。
【００１３】
基準電圧部１の出力する基準電圧レベルと、反転増幅部２の論理閾値電圧（基準電圧レベル）とが同一となるよう、ＰチャネルＭＯＳトランジスタＭＰ１及びＮチャネルＭＯＳトランジスタＭＮ１とのトランジスタサイズと、ＰチャネルＭＯＳトランジスタＭＰ２及びＮチャネルＭＯＳトランジスタＭＮ２のトランジスタサイズとが設定されている。
また、製造バラツキを考慮すると、好ましくは、基準電圧部１及び反転増幅部２との基準電圧レベルが一致するように、ＰチャネルＭＯＳトランジスタＭＰ１及びＰチャネルＭＯＳトランジスタＭＰ２のトランジスタサイズが同一であり、かつＮチャネルＭＯＳトランジスタＭＮ１及びＮチャネルＭＯＳトランジスタＭＮ２のトランジスタが同一となるよう設定する。
【００１４】
ＮチャネルＭＯＳトランジスタＭＮ３は、ＰチャネルＭＯＳトランジスタＭＰ１のドレインとＮチャネルＭＯＳトランジスタＭＮ１のドレインとの接続点Ａに一端（ドレインまたはソースのいずれか、例えば、ドレイン）が、ＰチャネルＭＯＳトランジスタＭＰ２のゲートとＮチャネルＭＯＳトランジスタＭＮ２のゲートとの接続点Ｂに他端（ドレインまたはソースのいずれか、例えば、ソース）が接続され、基準電圧部１及び反転増幅部２との間に介挿されたトランスファーゲートである。
【００１５】
上記ＮチャネルＭＯＳトランジスタＮ３は、ゲートに入力される制御信号によりオン／オフ制御され、制御信号が「Ｈ」レベルであるオン状態の場合に、基準電圧部１の出力する基準電圧を反転増幅部２の接続点Ｂに対して転送し、制御信号が「Ｌ」レベルであるオフ状態の場合、オフ状態となった時点の電圧値を容量４に保持する。
容量４は、コンデンサを設けても良いが、ＮチャネルＭＯＳトランジスタの他端の拡散層の容量、ＰチャネルＭＯＳトランジスタＭＰ２及びＮチャネルＭＯＳトランジスタＭＮ２それぞれのゲートの容量にて形成された寄生容量を用いても良い。
【００１６】
図１の反転増幅部２の入力電圧と、出力電圧との関係を図２を用いて説明する。
ＰチャネルＭＯＳトランジスタＭＰ２のゲートとＮチャネルＭＯＳトランジスタＭＮ２のゲートとの接続点Ｂには、ＮチャネルＭＯＳトランジスタＭＮ３を介して、基準電圧部１から基準電圧Ｖinが入力される。この基準電圧Ｖinは、反転増幅部２の論理閾値電圧（基準電圧レベル）と同一の値であり、熱雑音による微少電圧ΔＶin（数十μＶ～数百μＶ）により不安定に、不規則に揺らいでいる。また、基準電圧レベルＶinとしては、微少電圧ΔＶinの揺らぎの中心であることから、通常、電源の電圧値と接地との中間の電圧に設定される。

反転増幅部２は、入力電圧Ｖin自体が自身の基準電圧レベルと同一のために増幅することがなく、基準電圧レベルからの揺らぎ成分である上記微少電圧ΔＶinを予め設定された増幅率にて反転増幅（例えば、数十倍～数百倍）し、増幅電圧ΔＶout（数μｍＶ～数十ｍＶ）として出力する。

【００１７】

ここで、反転増幅部２は、微少電圧ΔＶinが小さく、高い周波数（例えば、１０ＭＨｚ）のため、応答ができない、すなわち反転増幅の動作を行えない。

そのため、ＮチャネルＭＯＳトランジスタＭＮ３を、ゲートに入力する制御信号を「Ｈ」レベルとしてオン状態にし、接続点Ｂの容量４に電荷を蓄積あるいは放電させて接続点Ａの電圧値を供給し、制御信号を「Ｌ」レベルとしてオフ状態とし、その時点の微少電圧ΔＶinを容量４サンプリングする。サンプリング周期としては、反転増幅部２の各ＭＯＳトランジスタにおける微少な電圧に対する応答速度を考慮して、低周波数（例えば、１Ｈｚ以上１００ｋＨｚ以下）を用いることが望ましい。

そして、反転増幅部２は、容量４に蓄積されている電荷に対応した電圧の反転増幅動作を行う。

【００１８】

次に、図３及び図４を用いて、図１の乱数発生回路の動作の説明を行う。図３は、シミュレーションに用いた回路の構成を示す図である。図４はシミュレーション結果を示す波形図であり、横軸が時刻、縦軸が電圧レベルを示している。ここで、シミュレータ としてはＨＳＰＩＣＥ（登録商標）を用いた。

また、シミュレーションに用いた図３の回路においては、図１におけるトランスファーゲートのＮチャネルＭＯＳトランジスタＭＮ３に換え、ＮチャネルＭＯＳトランジスタＭＮ４及びＰチャネルＭＯＳトランジスタＭＰ３を用いた双方向トランスファーゲート５を用いている。ＰチャネルＭＯＳトランジスタＭＰ３のソースとＮチャネルＭＯＳトランジスタＭＮ４のドレインとを接続点Ｄにて接続し、ＰチャネルＭＯＳトランジスタＭＰ３のドレインとＮチャネルＭＯＳトランジスタＭＮ４のソースとを接続点Ｅにて接続している。

【００１９】

接続点ＥにＭＯＳトランジスタにより形成した容量４を接続し、さらに接続点Ｅを反転増幅部２における接続点Ｂに接続している。

また、双方向トランスファーゲート５の接続点Ｄを図示しない基準電圧部１の接続点Ａに接続している。すなわち、双方向トランスファーゲート５の一端である接続点Ｄを基準電圧部１の出力端子である接続点Ａへ接続し、双方向トランスファーゲート５の他端である接続点Ｅを反転増幅部２の入力端子である接続点Ｂに接続している。

【００２０】

図２では、基準電圧部１を省略して、シミュレータの信号源から基準電圧（入力電圧）Ｖinを１．８９７５として、微少電圧ΔＶinを±５００μＶとして、三角波の列信号としてＮＯＩＳＥ信号を、双方向トランスファーゲート５の接続部Ｅに入力している。このとき、反転増幅部２の論理閾値電圧も、基準電圧Ｖinと同一の１．８９７５Ｖに設定されている。

また、双方向トランスファーゲート５のオン／オフを制御する制御信号Ｉnを、インバータＩＮＶ１及びインバータＩＮＶ２により、ＰチャネルＭＯＳトランジスタＭＰ３及びＮチャネルＭＯＳトランジスタＭＮ４各々のゲートに印加している。

【００２１】

制御信号Ｉnが「Ｈ」レベルのとき、インバータＩＮＶ１により「Ｌ」レベルの信号がＰチャネルＭＯＳトランジスタＭＰ３のゲートに印加され、インバータＩＮＶ１及びＩＮＶ２により「Ｈ」レベルの信号がＮチャネルＭＯＳトランジスタＭＮ４に印加され、双方向トランスファーゲート５が導通状態（オン状態）となる。

一方、制御信号Ｉnが「Ｌ」レベルのとき、インバータＩＮＶ１により「Ｈ」レベルの信号がＰチャネルＭＯＳトランジスタＭＰ３のゲートに印加され、インバータＩＮＶ１及

びＩＮＶ２により「Ｌ」レベルの信号がＮチャネルＭＯＳトランジスタＭＮ４に印加され、双方向トランスファーゲート５が非導通状態（オフ状態）となる。

【００２２】

次に、図４により、乱数発生回路の動作説明を行う。

上段の波形は接続部Ａから出力される微少電圧ΔＶinの揺らぎを有する基準電圧の波形を示している。基準電圧Ｖinが１．８９７５Ｖであり、この基準電圧レベルに対して微少電圧ΔＶinが５００μＶとしての揺らぎが、周波数１．５ＭＨｚの三角波のパルス列として重畳している。

中断の信号Ｉnは周期が２０μ秒、すなわち周波数５０ｋＨｚの、デューティ５０％パルス列（「Ｈ」レベル：５．０Ｖ、「Ｌ」レベル：接地電圧（０Ｖ））として入力されている。

下段の信号Outは、反転増幅回路２が容量４に蓄積された電圧の反転増幅結果の出力電圧レベルを示している。

【００２３】

時刻ｔ1において、制御信号Ｉnが「Ｌ」レベルから「Ｈ」レベルに遷移する。これにより、双方向トランスファーゲート５がオン状態となり、微少電圧ΔＶinの揺らぎを有する基準電圧Ｖinが容量４及び接続点Bに印加される。

このとき、微少電圧ΔＶinの揺らぎの周波数が反転増幅部２の応答速度より早いため、反転増幅部２の出力電圧Ｖ0outは、基準電圧レベルの１．８９７５Ｖにて出力されている。

【００２４】

次に、時刻ｔ2において、制御信号Ｉnが「Ｈ」レベルから「Ｌ」レベルに遷移する。これにより、双方向トランスファーゲート５がオフ状態となり、微少電圧ΔＶinの揺らぎを有する基準電圧Ｖinが容量４及び接続点Bに印加されず、「Ｌ」レベルに遷移した時点に容量４に印加されていた電圧レベルが保持される。

そして、反転増幅部２は、容量４に蓄積されている電圧を増幅して出力電圧Ｖ0outとして出力する。

このとき、応答速度によらず、反転増幅部２が容量４に蓄積されている微少電圧ΔＶinを増幅するため、反転増幅部２の出力電圧Ｖ0outは、基準電圧レベルの１．８９７５Ｖに対して、約１００ｍＶのΔＶ0outが重畳された電圧として出力されている。

【００２５】

時刻ｔ3において、制御信号Ｉnが「Ｌ」レベルから「Ｈ」レベルに遷移する。これにより、双方向トランスファーゲート５がオン状態となり、微少電圧ΔＶinの揺らぎを有する基準電圧Ｖinが容量４及び接続点Bに印加される。

このとき、微少電圧ΔＶinの揺らぎの周波数が反転増幅部２の応答速度より早いため、反転増幅部２の出力電圧Ｖ0outは、基準電圧レベルの１．８９７５Ｖにて出力される。

上述した処理が制御信号Ｉnの「Ｈ」レベル及び「Ｌ」レベル間の遷移により繰り返され、乱数としての出力電圧Ｖ0outが、双方向トランスファーゲート５のオフ状態の際に取り出すことができる。

【００２６】

この後、この出力電圧Ｖ0outをそのままＡ／Ｄ変換して、得られたビット列を乱数として用いても良いし、さらにΔＶ0outをフィルタにより取り出し、このΔＶ0outを増幅した後にＡ／Ｄ変換して得られたビット列を乱数として用いてもよい。

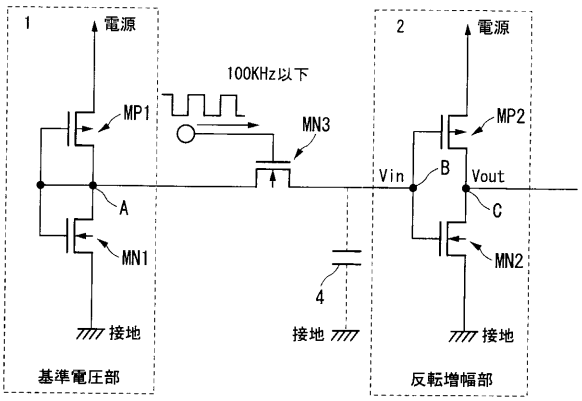
上述した本実施形態の構成により、熱雑音の微少電圧より物理的乱数を得る乱数発生回路を、ＣＭＯＳインバータ１個による基準電圧部１と、同様にＣＭＯＳインバータ１個による反転増幅部２からなる簡易な回路により実現することができるため、従来例に比較して回路を構成する面積を削減することができ、乱数発生回路を設けるチップの製造コストを減少させることが可能となる。

【図面の簡単な説明】

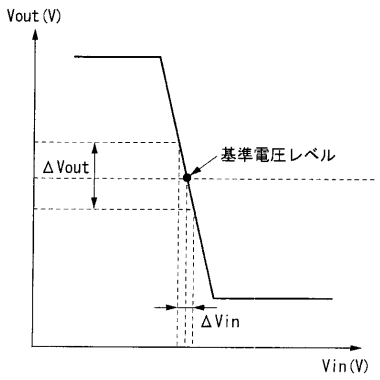
【００２７】

【図１】本発明の一実施形態による乱数発生回路の回路構成例を示す図である。
【図２】図１の反転増幅部１の増幅特性を示す、入力電圧（横軸）と出力電圧（縦軸）との対応関係を示すグラフである。
【図３】シミュレーションに用いた図１の乱数発生回路の回路構成を示す図である。
【図４】図３の乱数発生回路によるシミュレーション結果を示す波形図である。
【符号の説明】
【００２８】
１…基準電圧部
２…反転増幅部
４…容量（コンデンサ）
５…双方向トランスファーゲート
ＩＮＶ１，ＩＮＶ２…インバータ
ＭＮ１、ＭＮ２，ＭＮ３，ＭＮ４…ＮチャネルＭＯＳトランジスタ
ＭＰ１、ＭＰ２、ＭＰ３…ＰチャネルＭＯＳトランジスタ

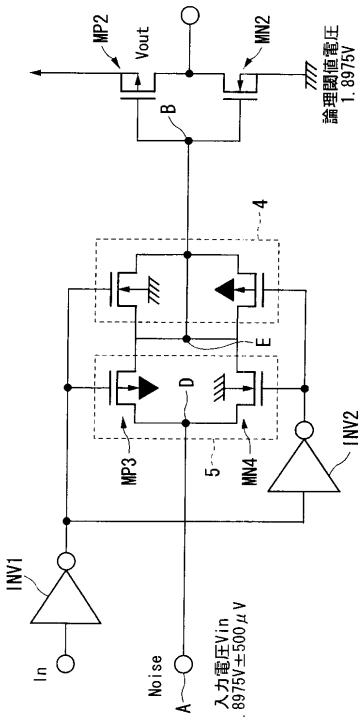
【図１】



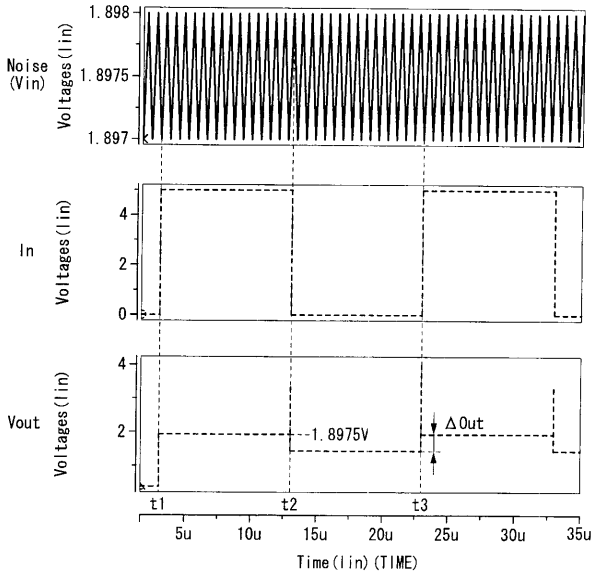
【図２】



【図３】



【図４】


Noise
(Vin)
Voltages(lin)
1.898
1.8975
1.897
In
Voltages(lin)
4
2
0
Vout
Voltages(lin)
4
2
1.8975V
ΔOut
t1
t2
t3
5u
10u
15u
20u
25u
30u
35u
Time(lin)(TIME)