CC-002

真性乱数発生器への利用を目的とした SR ラッチのメタスタビリティ解析

Metastability Analysis of SR-Latch for Application to a True Random Number Generator

前久 智哉† 籠谷裕人†
Tomoya Maehisa Hiroto Kagotani

1. はじめに

近年，通信技術の普及にともない，コンピュータセキュリティは不可欠となっているため，その基盤のひとつである真性乱数発生器（TRNG）は重要な要素である．特に暗号技術では疑似乱数発生器（PRNG）のシード，秘密鍵，パディング等の生成に TRNG を用いて予測不可能な値を使用することが望ましい．このことから効率的な TRNG の構成が多くの実用的なシステムで重要となる．

TRNG は一般的に熱雑音，量子揺らぎなどに基づいた仕組みで設計される．そのため，それらの TRNG はアナログ回路で構成されるが，FPGA 等のデジタル回路のみで構成されたデバイスで TRNG が必要な場合がある．そのような中で，SR ラッチやフリップフロップ回路でメタスタビリティを用いて，デジタル回路のみで構成した TRNG の研究がある．

典型的なメタスタビリティは同期回路の故障要因として扱われるため，発生を防ぎ，正常な動作を保証するための研究が多数ある．一方で，TRNG への利用のようにメタスタビリティを意図的に発生させる研究は少なく，特性について詳細に知られていないため，回路で使用されるトランジスタのパラメータ構成とメタスタビリティの因果関係が不明瞭なまま実装されている．このような背景からメタスタビリティを応用した技術の実用性を向上させることを目標に，本論文では CMOS 回路におけるメタスタビリティに対するトランジスタパラメータの影響のうち，メタスタビリティの容易性に関わるメタスタビリティ継続時間についてシミュレーションによって解析し，結果を報告する．

2. 基礎知識

2.1 物理現象におけるメタスタビリティ

物理現象におけるメタステーブル状態は，図 1 のようにボールと山で表すことができる．山の両側は安定状態を表している．山に向かってボールを投げるとき，十分な力を与えれば頂上の反対側に到達する．他方で，十分な力を与えなければ元の場所に転がり落ちてしまう．しかし，中間的な力でボールを投げちょうど山頂に着地した場合，安定状態ではないがそこで停止してしまうこともある．これをメタステーブル（準安定）状態という．メタステーブル状態は長時間続くことがあるが，風などの外的要因によって停止している状態から傾き，最終的にどちらかの安定状態に落ち着く．

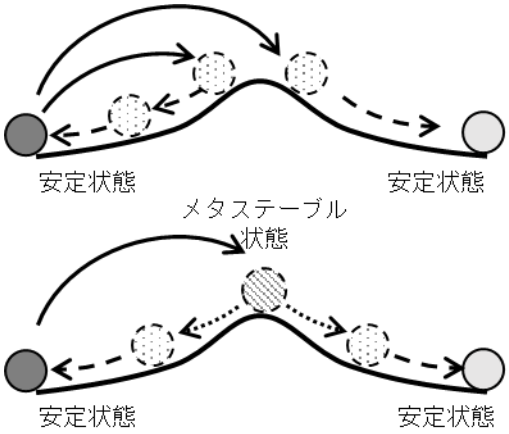

図 1 一般的な物理現象におけるメタスタビリティ

2.2 デジタル回路におけるメタステーブル状態

デジタル回路ではデータを保持するレジスタの各ビットにフリップフロップが使用される．フリップフロップはクロック信号の変化時点での入力信号値を取り込むので，その時点までに入力信号が安定している必要がある．図 2 に示すように，クロックエッジより前に安定していなければならない時間をセットアップ時間（t_{SU}），それより後に安定させ続ける必要のある時間をホールド時間（t_H）という．

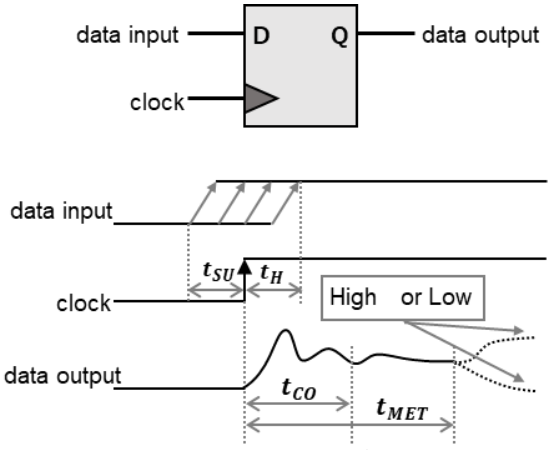

図 2 FF でのメタスタビリティ

これらの要求に違反した場合，デジタル回路もメタステーブル状態になる可能性がある．デジタル回路においてのメタステーブル状態とは，本来想定されているクロックエッジから出力が安定するまでの時間t_{CO} を超えても出力が安定していない状態と定義できる．実際に出力が安定するまでに必要な時間t_{MET} は，回路特性や周囲の雑音によって変動する．このような回路の特性はメタスタビリティと呼

† 岡山大学 Okayama University

ばれる．このことが要因でシステムに一時的な障害をもたらす場合もある．

2.3 NAND 型 SR ラッチにおけるメタスタビリティ

SR ラッチの場合、R 入力と S 入力の両方をアクティブにすることは一般的に禁止されている。この状態で両入力を同時に非アクティブにすると、SR ラッチがメタステーブル状態になり、不安定な出力を生成する可能性がある．図 3 は、メタスタビリティを意図的に持たせたラッチ構成である． IN = 0 のとき、このラッチは（Q、$\overline{Q}$）=（1,1）で安定し， IN = 1 にトグルすると、高確率でメタステーブル状態を経由して，（Q,$\overline{Q}$）=（1,0）または（0,1）のいずれかで安定する。

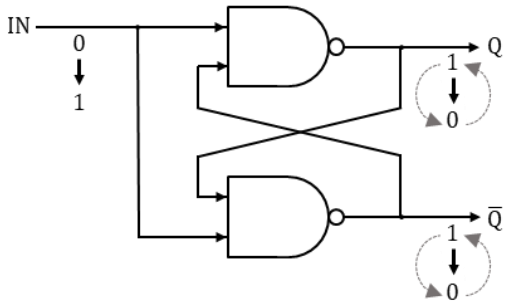

図 3　NAND ゲートでのメタスタビリティ

2.4 MOS トランジスタの特性

N 型 MOSFET における各部の電圧と電流を図 4 のように定義すると，これらの関係は式 1 のように表すことができる．各パラメータの意味は表 1 のとおりである． P 型 MOSFET においてもほぼ同様の性質である．

表 1　MOSFET パラメータの定義

記号	定義
KP	トランスコンダクタンス
V_T	スレショルド電圧
λ	チャネル長変調係数

$$I_{DS}=\begin{cases} KP\left\{(V_{GS}-V_T)V_{DS}-\frac{{V_{DS}}^2}{2}\right\}(V_{DS}\le V_{GS}-V_T) \\ \frac{1}{2}KP\{(V_{GS}-V_T)^2(1+\lambda V_{SD})-\lambda(V_{GS}-V_T)^3\}(V_{DS}\le V_{GS}-V_T) \\ 0(V_{GS}\le 0) \end{cases} \quad (1)$$

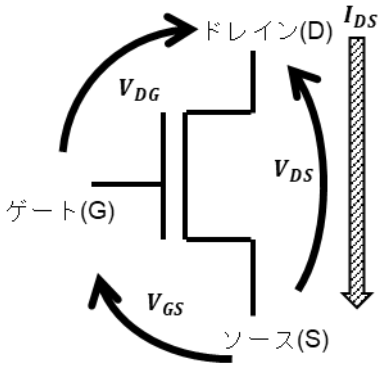

図 4　MOSFET 内での電圧と電流

3. SPICE を用いた SR ラッチの過渡解析

3.1 シミュレーション条件

本シミュレーションでは，SR ラッチのメタスタビリティ継続時間をメタスタビリティの起こりやすさとして評価する．また，メタスタビリティ継続時間は，それが長いほどノイズの影響をより多く受けることができ，予測困難性が増すため，メタスタビリティを TRNG 等に利用するにあたって重要な数値となる．

SR ラッチの両出力の電圧差をΔVとして扱い，$\Delta V < 3/5V_{dd}$ を満たす時間をメタスタビリティ継続時間Δtとして扱う．また，電源電圧V_{dd}としては 5V を用いた．

過渡解析を行うにあたって，NAND ゲートを図 5 に示す CMOS に置き換えてシミュレーションを行った．使用した SPICE モデルは付録に示す．

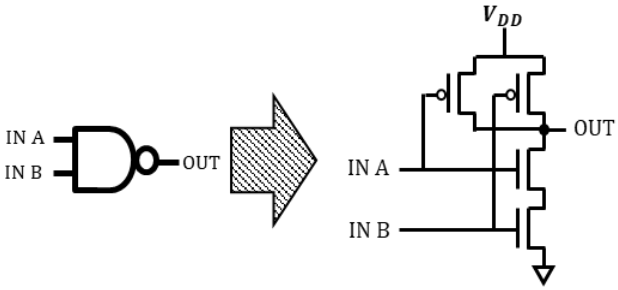

図 5　NAND ゲートの CMOS モデル

3.2 入力遅延差とメタスタビリティ継続時間

回路構成を図 6 に示す．SR ラッチにおいて意図的にメタスタビリティを発生させるために，入力 IN = 0 から IN =V_{dd} へトグルする．実際の回路において，完全に同じタイミングでのトグルはできないため，IN から NAND ゲートに流入するまでの遅延をD_1，D_2としてモデル化した．トグル入力の遅延差Dを$D_2 - D_1$として扱い，メタスタビリティ継続時間との比較を行う．

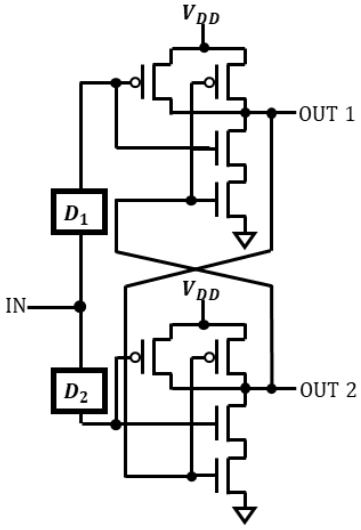

図 6　NAND 型 SR ラッチ回路

3.2.1 シミュレーション結果

SR ラッチにおける遅延差Dとメタスタビリティ継続時間との関係を図 7 に示す．これより，入力遅延差が 0 に近いほどメタスタビリティ継続時間が長いことがわかる．また，入力遅延差が正の場合を片対数グラフで図 8 に示す．この図において，入力遅延差がおよそ0.2μs未満は指数的な変化となっていることがわかる．

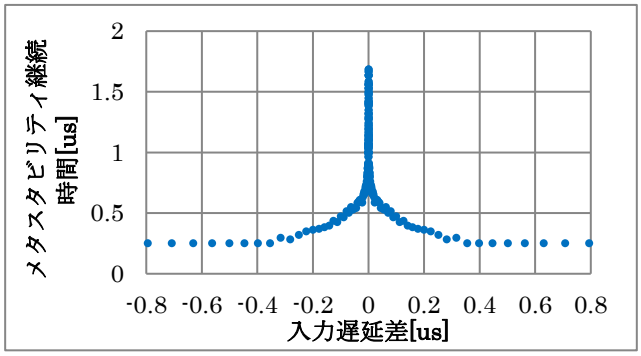

図 7　NAND 型 SR ラッチにおけるメタスタビリティ継続時間と入力遅延差

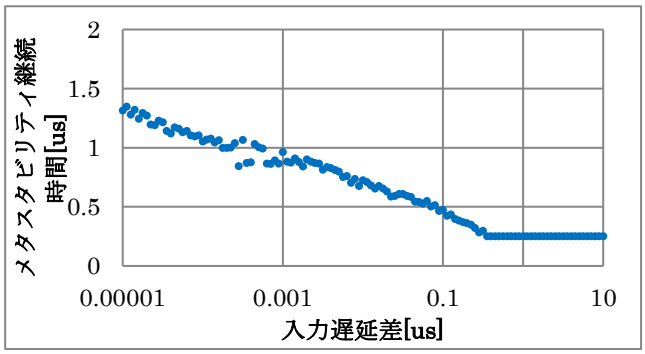

図 8　NAND 型 SR ラッチにおけるメタスタビリティ継続時間と入力遅延差（片対数）

3.3 NAND ゲートの入力パターンのメタスタビリティへの影響

3.3.1 SR ラッチの接続パターン

図 5 のような一般的な CMOS NAND ゲートでは 2 つの入力は対称ではない．図 9 に示すように，それぞれの NAND が 2 つの接続パターンを持っているため，1 つの SR ラッチにつき 4 パターンの接続方法がある．

OUT 1 と A を接続するパターンを 1-A と表記し，他の場合も同様に表記する．(1-A,2-A)を AA 接続，(1-B,2-B)を BB 接続，(1-A,2-B)を AB 接続，(1-B,2-A)を BA 接続と名づける．AA 接続と BB 接続は電気的に対称である一方で，AB 接続と BA 接続は電気的に非対称である．また，AB 接続と BA 接続は OUT1 と OUT2 を交換すれば等価であるので AB 接続のみを取り扱う．

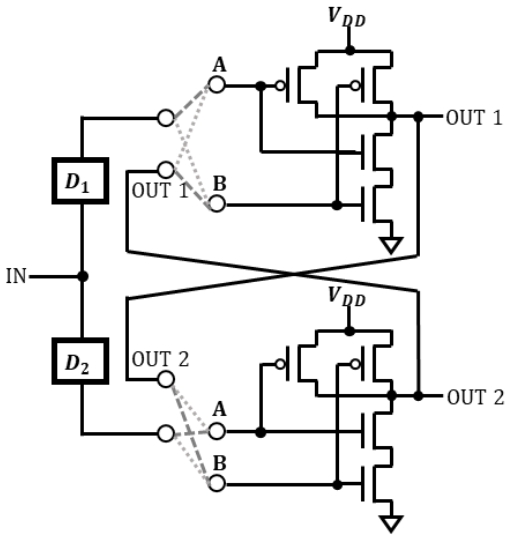

図 9　NAND 型 SR ラッチへの帰還とトグルの接続パターン

3.3.2 シミュレーション結果

上記した接続方法ごとのメタスタビリティ継続時間と入力遅延差との関係についてシミュレーションを行った．

それぞれの接続パターンによる遅延差Dとメタスタビリティ継続時間との関係を図 10 に示す．これは，接続が

図 10 より，AA 接続，BB 接続は，いずれも遅延差が0μs付近にピークがあり，メタスタビリティ継続時間のみが異なる．また，AB 接続においては，継続時間がピークとなる遅延差が0μs地点からシフトしていることがわかる．これは接続パターンにより電気的な非対称性からくるものと考えられる．

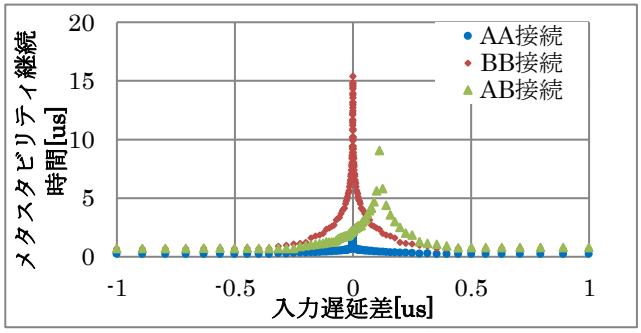

図 10　接続パターンによるメタスタビリティ継続時間と入力遅延差の変化

3.4 トランジスタパラメータと最大入力遅延差メタスタビリティ継続時間

トランジスタパラメータとメタスタビリティの関係を調べるため，トランジスタパラメータV_T, KP をそれぞれ典型値の 0.8 倍，1 倍，1.2 倍に変化させ，メタスタビリティ継続時間の特性の変化についてシミュレーションを行った．

3.4.1 シミュレーション結果

NMOS のKPパラメータを典型値の 0.8 倍，1 倍，1.2 倍に設定した場合の最大入力遅延差メタスタビリティ継続時間のそれぞれのグラフを図 11 に示す．

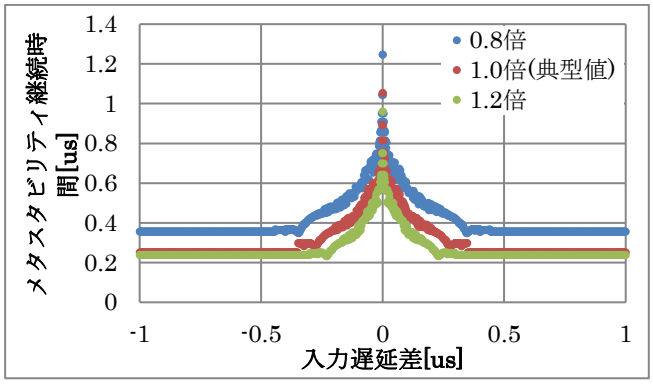

図 11　NMOS のKPパラメータを変化させた時の最大入力遅延差メタスタビリティ継続時間の変化

図より，パラメータの変動によりプロットが継続時間軸方向にシフトしている．同様の結果がV_Tについても見られ，また，PMOS でも同様であった．表 2 にパラメータを 0.8 倍，1.2 倍にした場合の典型値でのプロットからのシフト幅を示す．

表 2　パラメータを変動させた場合のプロットのシフト幅

パラメータ	シフト幅[ns]	
	0.8 倍	1.2 倍
PMOS KP	+33	-1
PMOS V_T	-3	+2
NMOS KP	+110	-36
NMOS V_T	-11	+20

これらの結果からメタスタビリティ継続時間は製造プロセスの際や動作時の温度等の影響を受けるものの，入力遅延差の小さい領域では相対的に影響は小さくなると言える．

3.5 トランジスタパラメータのばらつきのメタスタビリティへの影響

実際の CMOS 回路において，製造プロセスのばらつきにより各トランジスタパラメータは異なる値をとなる．ばらついたパラメータをシミュレーションするにあたって，平均に対する標準偏差の比を表す変動係数 CV (Coefficient of Variation)を用いる．平均値には各パラメータの典型値を用い，CV から算出される標準偏差を持つ正規分布により値を測定する．本シミュレーションでは，CV=0.01 として，1000 回シミュレーションを行い，メタスタビリティ継続時間がピークとなる入力遅延差をそれぞれ計算し，分布を調べる．また，この

3.5.1 シミュレーション結果

ばらつきを CV=0.01 としたときの，メタスタビリティ継続時間のピークの分布を図 12 に示す．図より，遅延差0μs 付近に一番多くピークが分布していることがわかる．また，この尖度は 1.8 であることから，正規分布よりも鋭く分布しており，ばらつきによるピーク位置の変動は大きくないと考えられる．

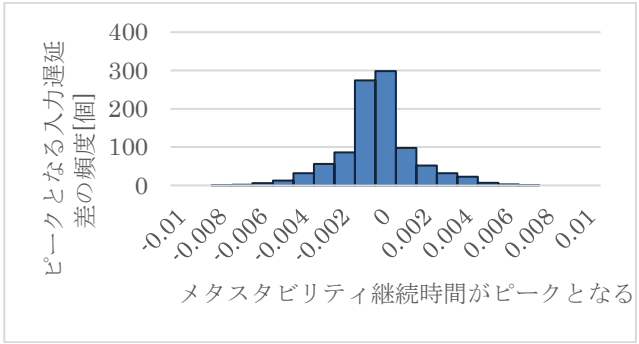

図 12　パラメータのばらつきにおけるメタスタビリティ継続時間のピークの分布

4. むすび

本論文では，メタスタビリティの性質を調査するために，NAND 型 SR ラッチにおけるメタスタビリティ継続時間とメタスタビリティ継続時間に関してシミュレーションを行った．

メタスタビリティ継続時間が最大となるピーク時間が存在することを解析した．また，そのピークは SR ラッチの NAND ゲートへの接続パターン，CMOS パラメータの変動により変化することが判明した．さらに，CMOS パラメータのプロセス誤差でのピークのばらつきも判明した．このピークを持つ遅延差は，SR ラッチでのメタスタビリティにおける出力の High および Low へどちらの出力が収束するかの条件と関係していると予測できる．そのため，メタスタビリティの出力の乱数性との関係を今後調査していきたい．

参考文献

[1] R.Giosar, “Metastability and Synchronizers: A Tutorial”, IEEE Design & Test of Computers, September/October, pp.23-35, (2011).
[2] 畑 尚志，“メタスタビリティを利用した真性乱数生成回路の FPGA による実装”，豊橋技術科学大学修士論文, (2008).
[3] R.J.Baker, “CMOS Circuit Design, Layout, and Simulation,” (2010).

付録

MOSFET パラメータの SPICE モデル

```
*SPICE LEVEL3 PARAMETESR
.MODEL NMOS NMOS LEVEL=3 PHI=0.7 TOX=9.5E-09
XJ=0.2U TPG=1 VTO=0.7 DELTA=8.8E-01 LD=5E-08
KP=1.56E-04 UO=420 THETA=2.3E-01 SRH=2.0E+00
GAMMA=0.62 NSUB=1.40E+17 NFS=7.20E+11
VMAX=1.8E+05 ETA=2.125E-02 KAPPA=1E-01
CGDO=3.0E-10 CGSO=3.0E-10 CGBO=4.5E-10
CJ=5.50E-04 MJ=0.6 CJSW=3E-10 MJSW=0.35 PB=1.1

*SPICE LEVEL3 PARAMETESR
.MODEL PMOS PMOS LEVEL=3 PHI=0.7 TOX=9.5E-09
XJ=0.2U TPG=-1 VTO=-0.95 DELTA=2.5E-01 LD=7E-08
KP=4.8E-05 UO=130 THETA=2.0E-01 SRH=2.5E+00
GAMMA=0.52 NSUB=1.0E+17 NFS=6.50E+11
VMAX=3.0E+05 ETA=2.5E-02 KAPPA=8.0E+00
CGDO=3.5E-10 CGSO=3.5E-10 CGBO=4.5E-10
CJ=9.50E-04 MJ=0.5 CJSW=2E-10 MJSW=0.25 PB=1
```