様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　２ 年　 ６ 月 １２ 日現在

機関番号：３２６８９
研究種目：基盤研究(C)（一般）
研究期間：2017～2019
課題番号：１７Ｋ０６４０４

研究課題名（和文）初期状態設定によるセキュリティー用自然由来データの高品質化の研究

研究課題名（英文）Quality Improvement of Natural Data for Security by Controling Initial State

研究代表者
篠原　尋史（Shinohara, Hirofumi）

早稲田大学・理工学術院（情報生産システム研究科・センター）・特任教授

研究者番号：５０５３１８１０

交付決定額（研究期間全体）：（直接経費）　　3,700,000円

研究成果の概要（和文）：モノのセキュリティーのため、自然由来乱数を生成する集積回路の品質向上を行った。基本構成のラッチ回路において、微小な素子ばらつきや熱雑音から安定して乱数を得るため、素子固有値を出力するPUFでは双安定の分水嶺から離れた点に初期状態を誘導し、毎回予測不能な値を生成するTRNGでは初期値を分水嶺上に設定するアイデアを用いた。
PUFでは、ホットキャリア注入によるミスマッチ強化などの技術で一層の安定性向上を図り、最悪の電源電圧・温度条件下やエージング後でエラーゼロを達成した。
TRNGでは、高出力効率の後処理回路と組み合わせて、6セル出力から1ビットの高品質乱数を安定して創出することに成功した。

研究成果の学術的意義や社会的意義
PUFは、暗号鍵の安全を守ることから信頼の礎と呼ばれている。従来は強力ECCで安定化していたが、回路が複雑で消費エネルギーも大きく、リアルタイム性にも乏しかった。本成果はECC不要なので、省エネルギー高速で、IoT端末適用が期待される。近年はゲート絶縁膜破壊や不揮発メモリを用いてエラーゼロの報告はある。標準CMOSプロセスで破壊痕跡なくエラーゼロを示した功績は大きい。
ラッチTRNGのコア回路は小さいが、出力が偏るためにフィードバック制御や多数のセルを準備する必要があった。本研究ではフィードバック制御無しに6セルだけから高品質乱数を得ることを実証したので、一層の小型省エネルギーに貢献できる。

研究成果の概要（英文）：Quality improvement of natural random data for IoT security has been done in this research. In order to obtain random number stably from weak natural signals e.g. device mismatch or thermal noise in the basic latch circuits, an idea to control the initial state is applied. In PUF, which generate device specific numbers constantly, the initial point is guided away from the dividing ridge for the final binary state. While in TRNG, which generate unpredictable number every time, the initial state is adjusted on the dividing ridge.
PUF have achieved no bit error without ECC under worst voltage and temperature corner conditions and after aging by further introducing mismatch enhancement technique through hot carrier injection.
Combination of TRNG and high output rate post processing circuit has successfully generated a high quality random bit with a rate of one bit from 6 TRNG cells raw outputs.

研究分野：集積回路、ハードウェアセキュリティ

キーワード：PUF　TRNG　乱数　ビットエラー率　ハードウェアセキュリティ

１．研究開始当初の背景

情報ネットワークの進展により、あらゆるモノがインターネットにつながって人々の生活や社会活動を豊かにする IoT 時代の到来が予想されている。これをセキュリティーの観点から眺めると、ハッキング対象が増大・拡散することに加えて、対象が人の関与が少ないモノであるという新要素が加わる。これを解決するにはモノの認証技術が必要である。更に IoT 端末は電源環境の悪いところにも設置されるので、エネルギー消費の少ないものが求められる。

自然由来の乱数を生成する PUF や TRNG は、コピーのしにくさや予測の困難性から、セキュリティー応用として国内外で研究されてきた。とりわけ SRAM を含むラッチタイプは、面積や消費電力の点で有利である。しかし、乱数の源となる自然信号は微弱で環境によって変化するため、生成データの品質面で課題があった。すなわち、PUF では熱雑音や温度変化の影響がセル固有のミスマッチより大きいとビットエラーが生じる。一方 TRNG では、ミスマッチが熱雑音と比べて無視できないため出力データが大きく偏る。これらの課題を克服するため、PUF では強力な ECC コードを用いたエラー訂正、TRNG では 2 重フィードバック制御や 256bit ラッチの XOR など重い後処理が必要で、回路が複雑になりエネルギー消費が大きい欠点があった。

２．研究の目的

本研究では、PUF, TRNG ともにラッチ回路を基本として、熱雑音の影響ややミスマッチを巧に取り除いたり強化したりすることにより、軽い後処理で高品質な自然由来の乱数を得ることである。これにより、ラッチ回路本来の省面積や低消費エネルギーを実現する。

３．研究の方法

本研究の中心をなす統一的考え方(アイデア)は、ラッチ回路の初期状態を調節してデータの出現確率を制御する点にある。即ち、ラッチ回路を構成する交差接続された 2 個のインバータのノード電圧を V_A,V_B とすると、(V_A, V_B)平面は最終的にデータが“１”または”0”の状態に落ち着く 2 つの領域に分けられて、その分水嶺が必ず存在する。PUF では、初期状態をセル固有ミスマッチに基づいて分水嶺から充分離れた点に誘導することで、エラーの無い安定な出力を得る。一方 TRNG では、セルにミスマッチがあってもそれに応じた分水嶺上に初期状態を設定することで、熱雑音をエントロピー源とするランダムな出力を得る。

PUF では、更に高電圧バーンインによるミスマッチの強化や潜在的不安定セルの検出とマスキングの手法を組み合わせて、ビットエラー率を研究開始時の世界水準よりも数桁低い 1E-7 にまで低減する。

TRNG では、出力の”1”出現確率に多少の偏り(バイアス)が生じることは避けられないので、これを効率よく取り除いて高品質乱数を生成する後処理回路を合わせて研究する。

４．研究成果

(1) EE SRAM PUF

ラッチの初期状態を分水嶺から離れたところに誘導するビットセルを複数検討したが、ここでは EE (Enhancement-Enhancement) SRAM PUF を報告する。

ビットセルは図１ に示す通り、負荷素子として nMOS(LL, LR)を用いた EE インバータの交差接続を基本ラッチ回路としている。EE インバータの入出力伝達特性は CMOS インバータと違って直線状で、ゲイン(傾き)は電源電圧とともに増大する。このためラッチ回路は、電源電圧を上昇させると、ゲインが 1 になる点を境として、バタフライ曲線(2 つの入出力伝達曲線を同じ電圧平面に描いたもの)の交点が 1 個の単安定状態から交点が 2 個の双安定状態へと変化する。しきい値電圧差 20mV のミスマッチを想定した時のシミュレーション結果図 2 に示す。V_{DD}=0.7V～0.9V の間は単安定で、V_{DD} 上昇と共に丸印で示した安定点(双安定になる前の初期状態)はミスマッチが増幅されるかたちで分水嶺(点線で示した V_B=V_A 線)から遠い左上に誘導される。この結果、V_{DD}=1.0V で双安定となって右下にもう一つの安定点(点線○印)が現れてもラッチの状態がそちらに移ることはなく、再現性の良い PUF 評価データが得られる。

130nm CMOS で試作した 1Kbit EE SRAM PUF 20 チップの標準条件でのビットエラー率(BER)と不安定セル率(エラー発生したセルの割合)の実測結果を図 3 に示す。BER は 0.21%で通常の SRAM PUF から 1/14 に低減されている。また不安定セル率 2.14%も通常 SRAM PUF の数分の一である。

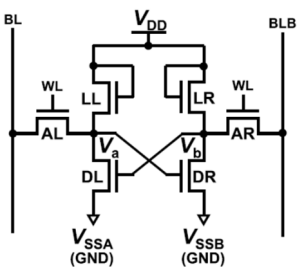

図 1.EE SRAM PUF ビットセル

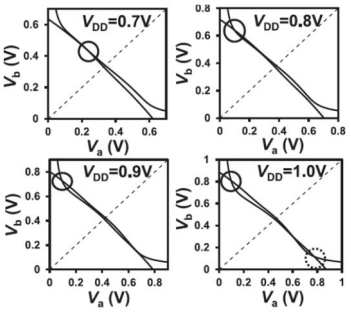

図 2.バタフライ曲線と安定点の推移

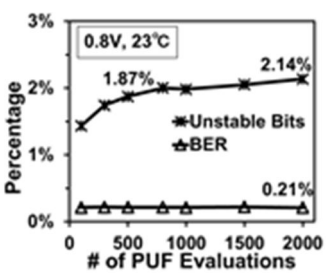

図 3.ビットエラー率と不安定セル率

(2) オンチップバイアス発生器を用いた EE SRAM PUF 安定化

EE SRAM PUF では、ミスマッチを増幅させる形で初期状態を分水嶺から離れたとことに誘導し、標準条件で低い BER を実現できた。しかし、電源電圧 V や温度 T が変化するとミスマッチそのものの極性が反転してデータ反転(常時ビットエラー)する課題が残されている。この課題を、潜在的不安定セルの検出とマスキングと、高電圧バーンインによるミスマッチ強化、の二つのアプローチで解決した。それぞれ本節(2)と次節(3)で報告する。

不安定セルをテストで検出してそれをマスクし、安定なセルだけを用いることでビットエラー率を小さくすることがマスキングの基本的な考えである。しかし、全条件でテストするのは、特に高温と低温でテストすることは、テストコスト増大を招く。そこで本研究では室温だけで潜在的不安定セルを効率よく検出する方法を開発した。潜在的不安定セル検出の概念を図 4 で説明する。図 4 左はミスマッチの分布を表していて、ゼロを中心にガウス分布をしている。ゼロ付近の斜め線部分が熱雑音で不安定になる不安定セル(図 3 の 2.14%に相当)で、その左右に温度や電圧を変化させて初めて現れる潜在的不安定セルが分布する。そこで、図 1 の V_{SSA} と V_{SSB} に電位差を与えて人工的ミスマッチを上乗せすることで分布を左右にシフトさせる(図 4 右は右シフトの場合)。これでデータが反転すると、潜在不安定セルに認定されてマスクされる。V_{SS} 電位差をオンチップで発生する回路を図 5 に示す。EE SRAM では nMOS 負荷は常時オンなので評価期間中貫通電流(I_{SC})が発生する。これが MOS トランジスタ M0～M7 を流れる時の電圧降下を V_{SS} 電位差に利用する。S1 と S2 の開閉を切り替えて両極性で評価する。また、M0～M8 のオン抵抗を変えることで、V_{SS} 電位差の絶対値を変化させる。絶対値が大きいと、多くの潜在不安定セルが検出されて、マスク率は高くなるが、厳選された安定セルが残って安定性が増す。

このオンチップ V_{SS} 電位差発生回路を用いて、室温で検出した潜在不安定セルをマスクし、温度や電源電圧条件が大きく離れた VT コーナでの有効性を実測で確認した。図 6 (a)(b)は、それぞれ 1.4V -40℃, 1.4V +120℃の VT コーナである。どちらの場合でも、マスク率を高めると共にビットエラー率が低下し、最終的に 67.4%のマスク率でエラーゼロを記録した。悲観的仮定として、次の測定でエラーが発生するとしてもビットエラー率は 1.50E-7 (=1/(3339bitx500 回 x4 コーナ))となる。 ECC 無しで、ほぼ目標のビットエラー率を達成した。なお、マスク率 67.4%では有効 bit は約 1/3 しかなくて、有効セル効率が低下している。マスク率を下げることは課題であるが、従来の SRAM PUF と ECC の組み合わせの場合は、有効セル効率は 10%程度しかなく、それに比べると 3 倍の改善である。

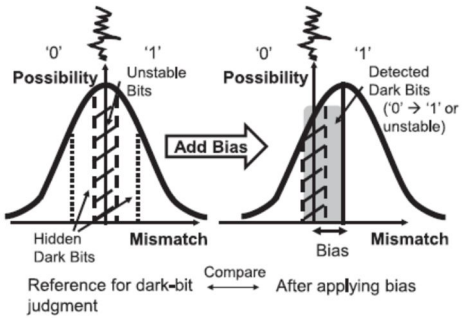

図 4. 潜在的不安定セル検出の概念

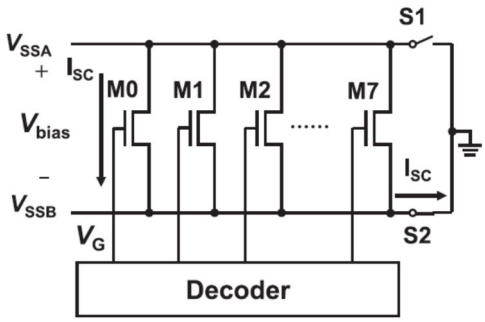

図 5. オンチップ V_{SS} 電位差発生回路

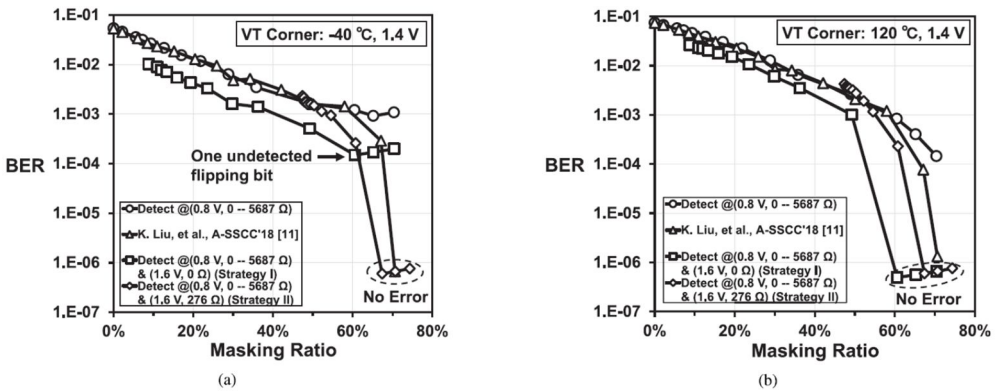

図 6. 電源電圧・温度コーナ条件でのビットエラー率 (a) 1.4V -40 ℃, (b) 1.4V +120℃

(3) EE/CMOS ハイブリッド SRAM PUF とホットエレクトロン注入による安定化

電源電圧 V や温度 T が変化しても安定な PUF を得るもう一つのアプローチとして、ホットエレクトロン注入 HCI (Hot Electron Injection) によるばらつき強化を行った。このアプローチは前節(2)における有効セル効率低下の解決策でもある、なお、他のバーンインとして NBTI(Negative Bias Temperature Instability) も試みたが、現在のところ HCI の方が良好な結果を得ることが出来たので、こちらを報告する。

HCI とは集積回路における長期使用時の特性変化の一要因で、ドレイン近傍の高電界で加速された電子がゲート絶縁膜に飛び込んで捕獲されることで、しきい値電圧 Vth が増大する現象を指す。ここでは、EE SRAM PUF ビットセルの一対の負荷 nMOS の片側だけに選択的に HCI を起こすことで、ミスマッチを増大させる。この概念を図 7 に示す。点線は図 4 左と同様に初期のミスマッチ分布示す。これの右半分即ちデータ”1”のビットセルには正のミスマッチ加えて右にシフトさせ、左半分即ちデータ”0”のビットセルには負のミスマッチを加えて左にシフトさせる。この結果、HCI 後のミスマッチの分布を太線のように 2 つのピークを持つ分布となり、中央の不安定セルや潜在的不安定セルを消滅させる。

選択的 HCI でミスマッチを強化する回路と方法を図 8 と図 9 で説明する。8 トランジスタから成るビットセルを図 8 に示す。EE SRAM と比べると pMOS P1, P2 が追加されている。P1,D1,P2,D2 に着目すると CMOS ラッチなので、EE と CMOS のハイブリッド構成である。PUF データ評価時は V_Pを 0V にして P1,P2 をオフさせて EE SRAM PUF として動作させる。その後 V_Pを電源電圧に、V_{NG}, V_{DG}を 0V にして CMOS SRAM に切り替え、安定読み出しをする。この EE から CMOS への切り替えは低エネルギー化にも有効である。HCI 時の動作を、PUF データが”1”の場合を例に、図 9 に示す。この場合 Q=”1”, QB=”0”なので、L1 と L2 のミスマッチに注目すると L2 の方が Vth 高くて充電能力が低いと考えられる。そこで L2 に選択的に HCI を起こす。HCI は MOS トランジスタのドレイン電圧の高い飽和状態の時に起きるので、SRAM ラッチに逆の”0”を書き込んで Q=”0”, QB=”1”としてから V_{NG}=0V とし V_Pに高電圧を印加する。青矢印で示した電流が流れ、L2 に HCI が起きる。L1 には電流が流れないか流れたとしてもリニア領域での動作なので HCI は起きない。この結果、元々高かった L2 の Vth だけが一層高くなり、Vth のミスマッチが強化される。

130nm CMOS プロセスで試作した 1Kbit ハイブリッド SRAM PUF の実測評価結果を図 10,図 11 に示す。図 10 はビットエラー率 BER の HCI バーンイン時間依存性である。標準条件 0.6V 25°C に対して 0.5V～0.7V, -40°C～+120°Cの 4 個の VT コーナでも、10 分間の HCI バーンインでエラーが 0 となった、前記の悲観的仮定での BER は、各コーナで 5E-7(=1/1Kbit x 500 回)、4 コーナ総合で 1.25E-7 である。更に 1.8V 125°Cでエージング加速試験を行った結果を図 11 に示す。通常条件の 21 年に相当する 60 時間後に、1 万回評価してもエラーは発生しなかった。これは同様に 1E-7 (=1/1Kbitx10k 回)に相当する。よって、目標を ECC 無しで達成した。しかも、VT コーナやエージング後の過酷な条件下である。近年、酸化膜破壊や不揮発メモリによるゼロ BER が報告されているが、破壊の痕跡を残すことから、PUF と呼べるのかと言った議論もある。本研究は(2)(3)共に、破壊の痕跡を残すことも、追加の製造プロセスもなく BER ゼロを達成したところに意義がある。

PUF データ生成と読み出しの消費エネルギーは、ハイブリッド化することで EE SRAM PUF よりも大幅に低下し、2.07fF/bit であった。これは、報告されている BER ゼロの中では最小で、他の BER が高いものを含めても 3 番目の小ささである。

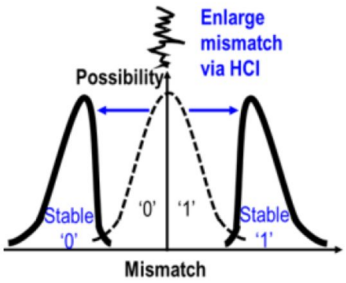

図 7.HCI によるミスマッチ強化概念

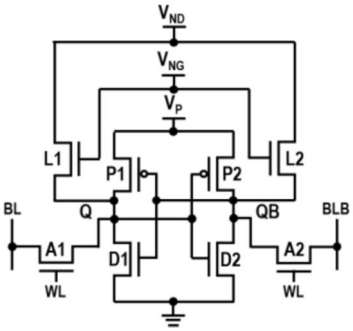

図 8.EE/CMOS ハイブリッド SRAM PUF ビットセル

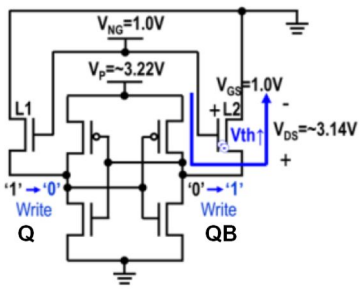

図 9.HCI 時の動作(L2 選択時)

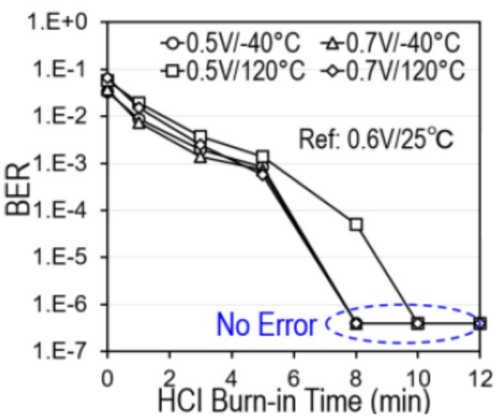

図 10. ビットエラー率 B の HCI バーンイン時間依存性

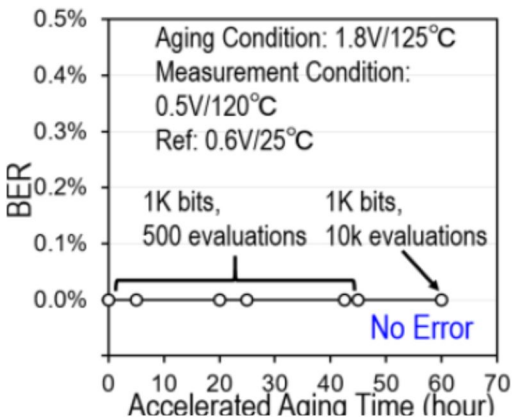

図 11. エージング加速試験結果

(4) ラッチ形 TRNG

ラッチ形 TRNG の動作原理を図 12 を用いて説明する。交差接続された二つのインバータの伝達特性(バタフライカーブ)は 3 個の交点 CP0，CP1，CPX を持つ。CP0，CP1 は安定点で、それぞれデータ”0”“1”に対応する。一方 CPX は不安定点である。素子ばらつきによって点線で示した分水嶺の位置は変化するが、CPX の位置も同様に変化し、分水嶺は常に CPX を通る。そこで初期状態を CPX に設定すれば、CP0 か CP1 のどちらに落ち着くかは熱雑音で左右されることになり、素子ばらつきや電源電圧変化の影響を受けることなく安定して乱数を得ることが出来る。この初期値設定には、スイッチトキャパシタ回路を用いる。

130nm CMOS で試作したラッチ形 TRNG の実測評価結果を図 13 に示す。これは 16 個の TRNG 出力の平均エントロピーで、0.8V から 1.5V の広い電源電圧範囲で 0.3bit 以上のエントロピーを得ることが出来た。6 個の TRNG 出力の合計は 1.8bit 以上となる。次節(5)に示す VN_8W 後処理の効率 62.2%を考慮すると 1.12bit 以上の高品質乱数が得られることになり、当初目標を達成した。また、VN8_W 後処理後の乱数は、NIST SP800-22 の 15 項目の乱数テスト全てにパスしている。

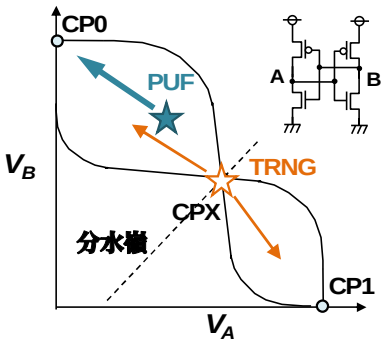

図 12.ラッチ形 TRNG 動作原理

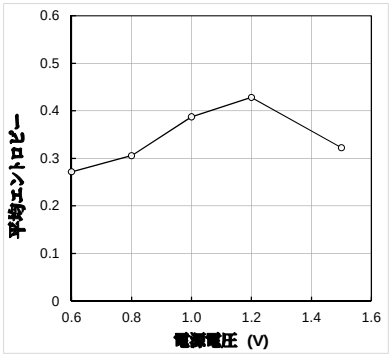

図 13.ラッチ形 TRNG 実測評価結果(16 個平均)

(5) N ビット von Neumann 後処理回路

乱数の”1”確率の偏り(バイアス)を除去するアルゴリズムとして von Neumann の方法が知られている。これは 2bit をペアにして(01)であれば”0”を(10)であれば”1”をそれぞれ出力し、(00)と(11)の場合は出力無しとするもので、簡単な回路でバイアス除去できるが、平均 4bit 入力に対して 1bit 出力しか得られないので出力効率は高々25%と低かった。

この効率を高めるために N bit まとめて処理する方法を用いた。N の増大とともに効率はシャノンエントロピーの限界に近づいて行くが、回路規模も大きくなる。そこで、小さな N でも高効率が得られるよう Waiting 方式を考案した。N=4 の場合の VN_4W を図 14 で説明する。16 通りの 4bit 入力を、(a)で色分けした通り”1”の数に応じて 5 個のグループ S0～S4 に分ける。S1 と S3 は要素数が各々4 個で、グルー内での出現確率が等しいので、(b)左と中に示す通り 2bit 出力を割り当てる。S2 の場合は要素数が 6 で 2 のべき乗ではないので、従来は 4+2 に分解してそれぞれ 2bit と 1bit を割り当てていた。しかし平均 1.67bit しか得られないので効率が悪い。そこで 6=2x3 に分解し、(b)右に示す通り 1bit と 3 進コード 1 個を割り当てる。この 3 進コードは次の 3 進コードが発生するまで Waiting し、2 個揃うと図 15 に示す通り 3bit または 0bit 出力する。これにより S2 の場合の平均出力は 2.33bit となり、出力効率が改善される。出力効率の N 依存性を図 16 に示す。赤線が Waiting ありの場合で、N=8 の VN_8W では 62.21%(入力バイアス無い場合)と、オリジナル von Neumann 法の約 2.49 倍に改善された。

VN_8W のロジック回路設計に際して、論理簡単化のため、入力選択による出力確定法と階層的設計の二つの技術を開発した。結果、P&R 後のゲート規模は 381GE に抑制出来た。また、内部動作周波数をデータ入力周波数の 1/8 に抑えることで、130nm CMOS スタンダードセルで、出力 1bit あたりのエネルギーは 3.12pJ/bit (@1.5V)であった。低電圧動作で 1pJ/bit 以下に出来ることが見込まれ、最先端の低エネルギーTRNG の後処理回路としての活用が期待出来る。

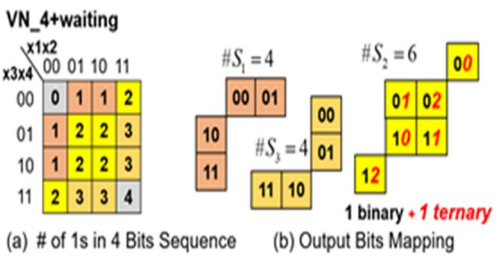

図 14. VN_4W の 出力コード割り当て

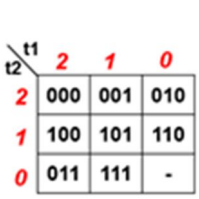

図 15. 2 個の 3 進数からのコード割り当て

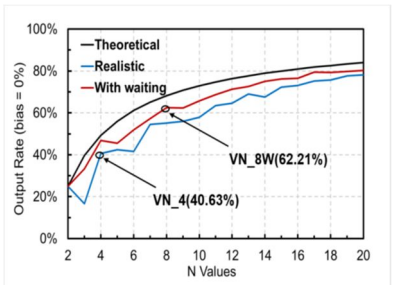

図 16.出力効率の N 依存性

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 Liu Kunyang、Min Yue、Yang Xuan、Sun Hanfeng、Shinohara Hirofumi	４．巻 55
２．論文標題 A 373-F? 0.21%-Native-BER EE SRAM Physically Unclonable Function With 2-D Power-Gated Bit Cells and VSS Bias-Based Dark-Bit Detection	５．発行年 2020年
３．雑誌名 IEEE Journal of Solid-State Circuits	６．最初と最後の頁 1719-1732
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/JSSC.2019.2963002	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計7件（うち招待講演　1件／うち国際学会　5件）

１．発表者名 Kunyang Liu, Yue Min, Xuan Yang, Hanfeng Sun and Hirofumi Shinohara
２．発表標題 A 373 F2 2D Power-Gated EE SRAM Physically Unclonable Function With Dark-Bit Detection Technique
３．学会等名 IEEE 2018 A-SSCC, pp.161-164, Nov. 2018.（国際学会）
４．発表年 2018年

１．発表者名 Ruilin Zhang, Sijia Chen, Chao Wan, Hirofumi Shinohara
２．発表標題 High-Throughput Von Neumann Post-Processing for Random Number Generator
３．学会等名 IEEE, 2018 International Symposium on VLSI Design, Automation and Test (VLSI-DAT), D3-1, April 2018.（国際学会）
４．発表年 2018年

１．発表者名 Xuanhao Zhang, Xiang Chen, Hanfeng Sun and, Hirofumi Shinohara
２．発表標題 Compensation of Temperature Induced Flipping-Bits in CMOS SRAM PUF by NMOS Body-Bias
３．学会等名 IEICE Technical Report, HWS2018-38, pp. 333-336, July 2018
４．発表年 2018年

１．発表者名
篠原尋史

２．発表標題
情報セキュリティのためのランダム回路

３．学会等名
信学技報、ICD2018-11, pp. 45-46, 2018年 4月（招待講演）

４．発表年
2018年

１．発表者名
Ruilin Zhang

２．発表標題
High-Throughput Von Neumann Post-Processing for Random Number Generator

３．学会等名
IEEE, International Symposium on VLSI Design, Automation and Test (VLSI-DAT)（国際学会）

４．発表年
2018年

１．発表者名
Kunyang Liu, Hongliang Pu and Hirofumi Shinohara

２．発表標題
A 0.5-V 2.07-fJ/b 497-F2 EE/CMOS Hybrid SRAM Physically Unclonable Function with < 1E-7 Bit Error Rate Achieved through Hot Carrier Injection Burn-in

３．学会等名
IEEE 2020 Custom Integrated Circuits Conf. ,p1-4, March 2020.（国際学会）

４．発表年
2020年

１．発表者名
Ruilin Zhang and Hirofumi Shinohara

２．発表標題
High-Throughput & Power Efficiency 8 Bits Von Neumann Post-Processing with Waiting Strategy for True Random Number Generators

３．学会等名
TJCAS 2019（国際学会）

４．発表年
2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究協力者	平本　俊郎 (Hiramoto Hoshiro)		