

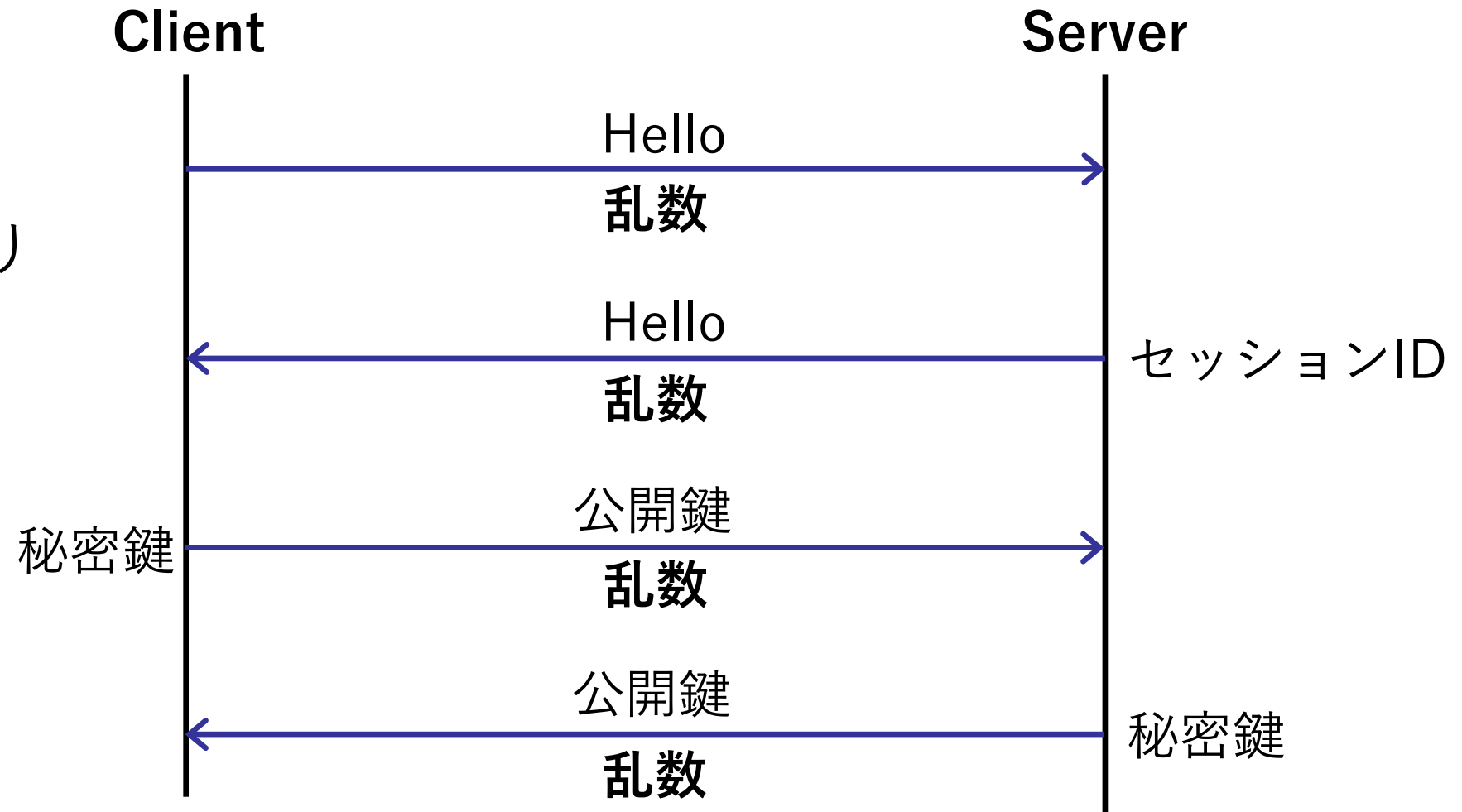
自律補償機構を備えた CMOS物理乱数発生回路

東京科学大学 工学院 情報通信系
准教授 イスラム マーフズル

2026年6月25日

乱数はセキュア通信に必要不可欠

インターネット通信
における最初のやり取り



- Websiteにアクセス毎にTLS 1.3 ハンドシェイク
- **4つ**の重要な**乱数**が生成される (256ビット以上)
- 他にも内部で乱数を生成

通信ごとに乱数が生成される

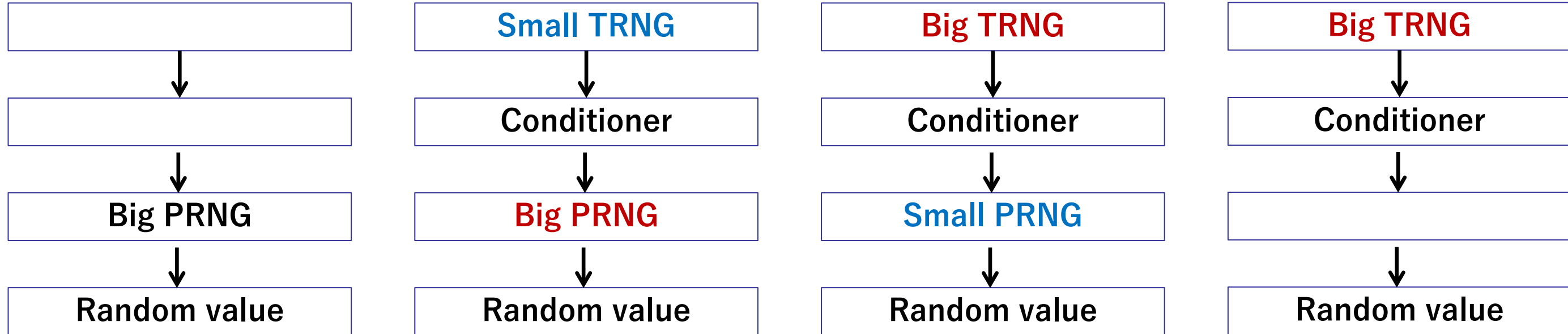
- **1000** TLS handshakes/s. $1000 \times 1024 \text{ bits} \approx \mathbf{1 \text{ Mbit}}$
- **~100** million web servers. $\mathbf{10^9}$ TLS handshakes/s
- $10^9 \times 10^6 = \mathbf{10^{15}}$ random bits/s

脆弱

弱い

強い

強靱



PRNG (Pseudo Random Number Generator : 擬似乱数生成器)
TRNG (True Random Number Generator : 真の乱数生成器)

- 世界中、秒ごとに10億以上の乱数が生成されている
- 強靱な通信には大量の高速なTRNGが必須

真の乱数生成回路(TRNG)の市場

□ TRNGの市場

- 2024年の売上はUSD **4.7** Billion
- 年間成長率**8.2%**
- 発振器(FRO)に基づいたTRNGが**50%**近く占有

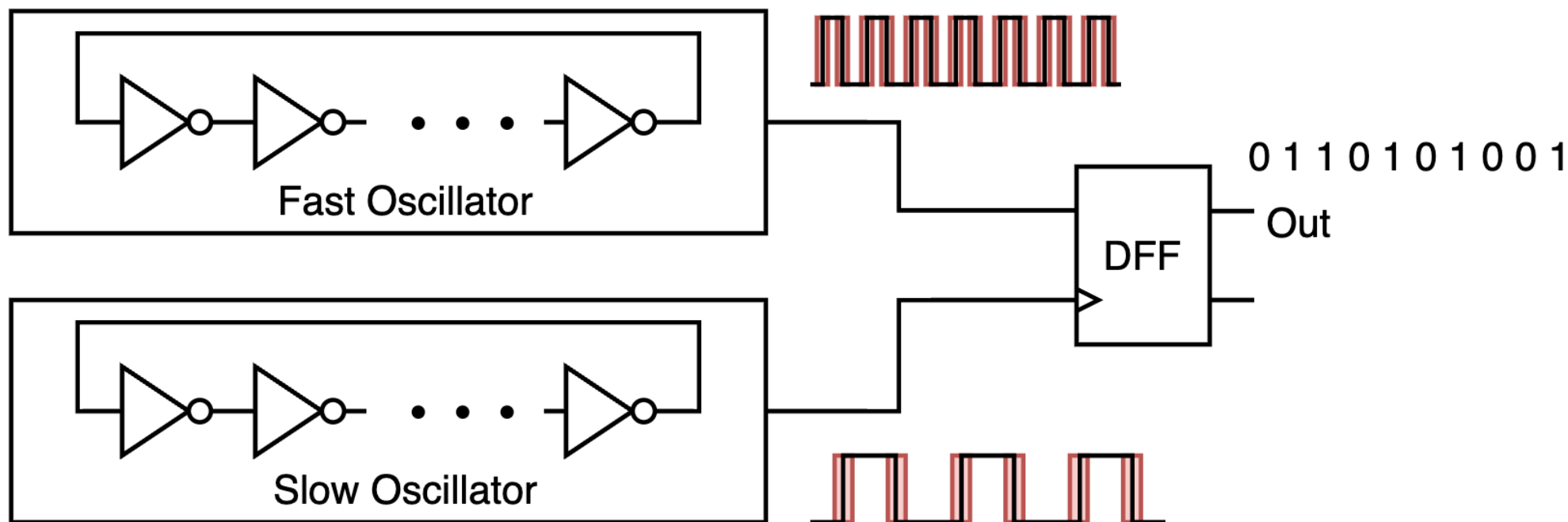
□ 電気回路方式によるTRNGの得失

- 発振器(FRO)によるTRNGの市場が大きい理由は**設計容易さ**である
⇒ **大面積で大消費電力**
- 電気ノイズによるTRNG
⇒ 現状では**設計困難**あるいは遅い
- **小面積と低消費電力と低設計コストの同時達成が課題**

従来技術①

発振器による乱数生成 (Synopsys社)

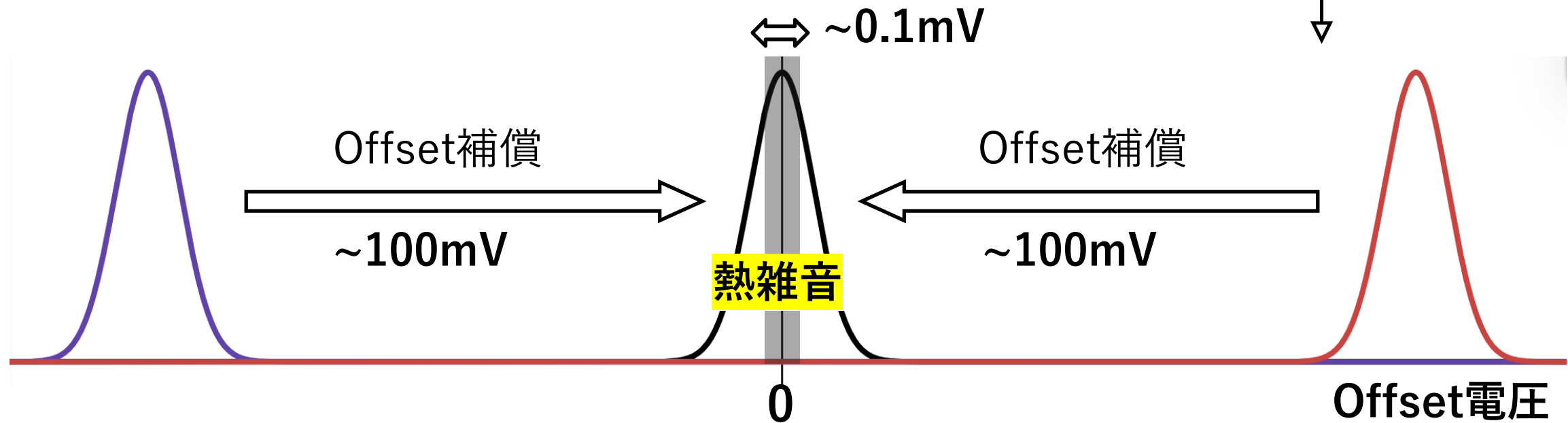
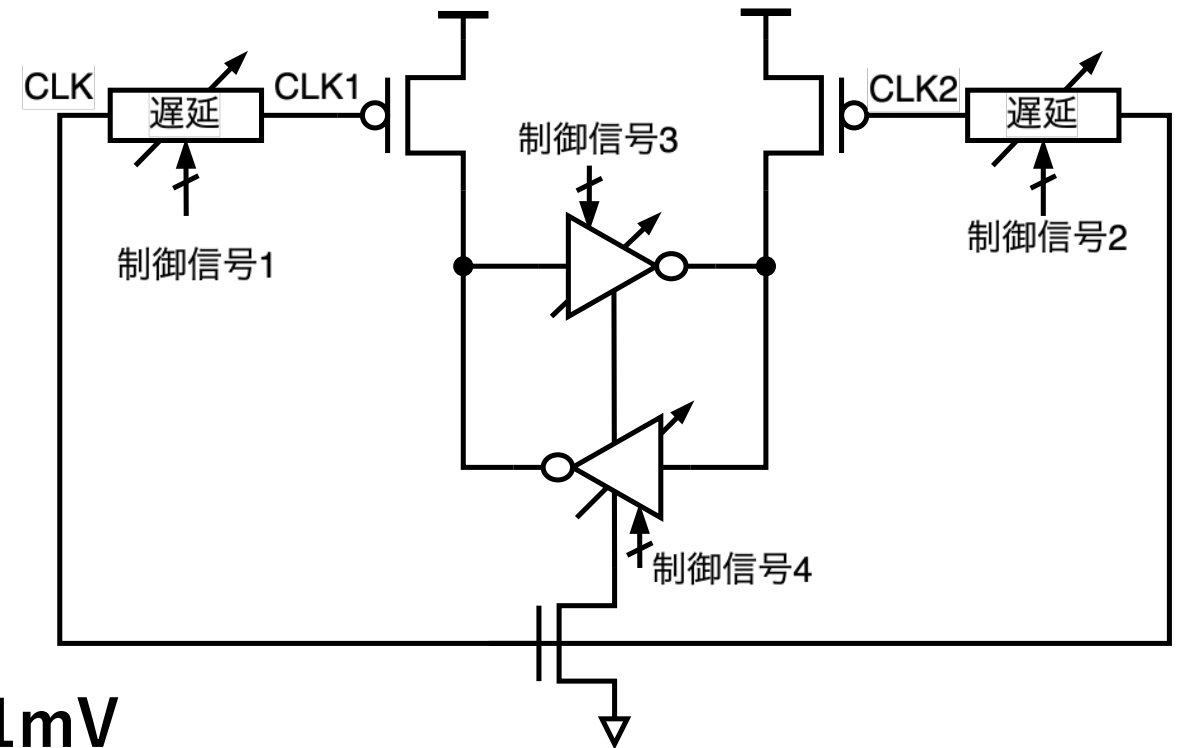
- リング発振回路 (RO) を複数利用
 - 設計しやすい 😊
 - 遅い** 😞
 - 電源ノイズや温度の影響を受けやすい 😞
- 周期的 ⇒ 後処理 ⇒ **大規模, 大消費電力**



従来技術②

ノイズによる乱数生成 (Intel)

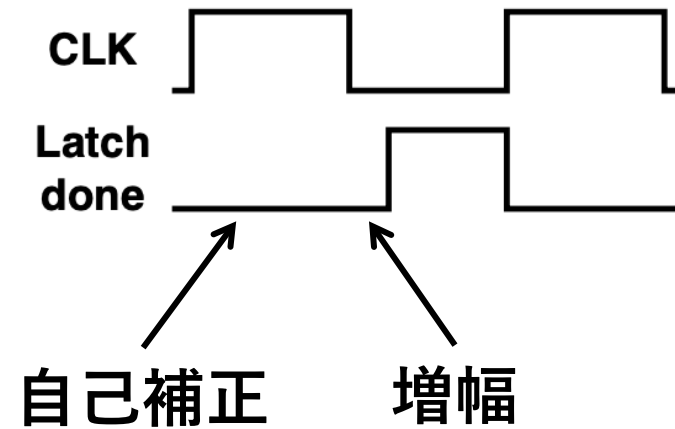
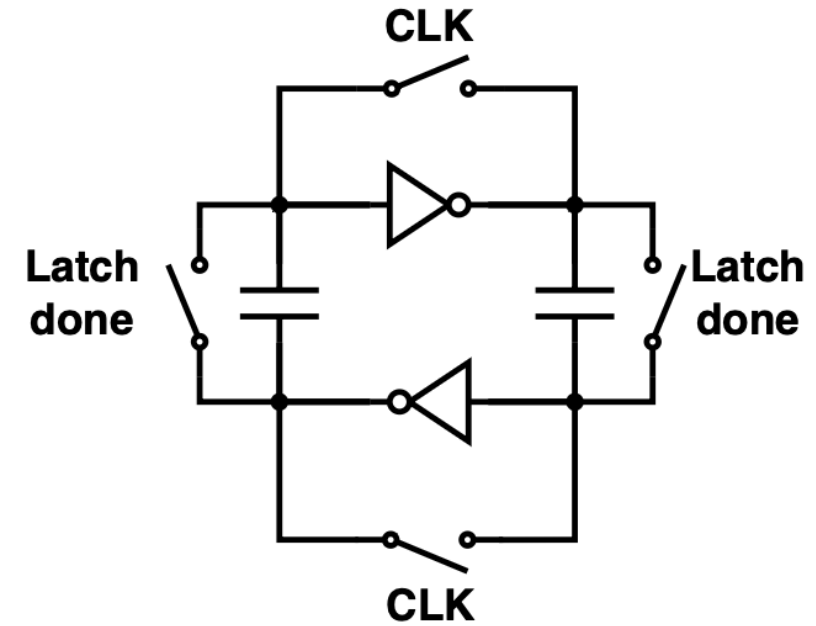
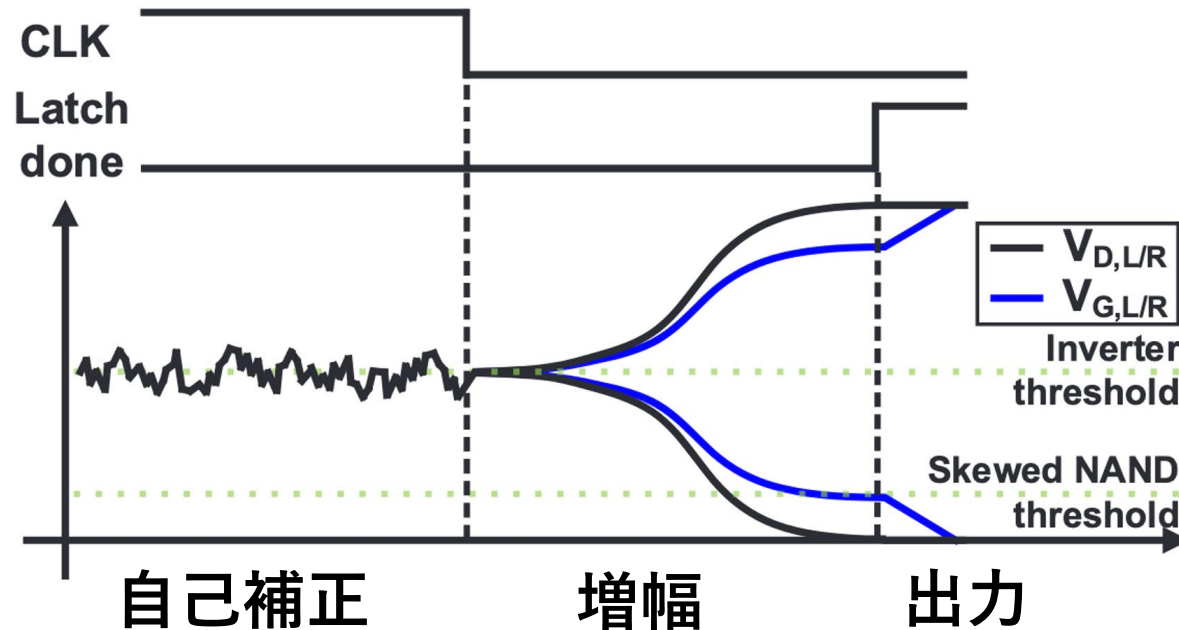
- 電気ノイズを直接デジタル値に変換
 - 設計が難しい 😞
 - 速い 😊
 - ばらつきの影響を受けやすい 😞
- 動的デジタルキャリブレーション
 - ⇒ 大面積, 大エネルギー 😞



従来技術③

ノイズによる乱数生成 (Samsung)

- 電気ノイズを直接デジタル値に変換
 - 設計が容易 😊
 - 遅い 😞
 - ばらつきの影響を相殺 😊
- 容量が大きい ⇒ **大面積, 遅い**



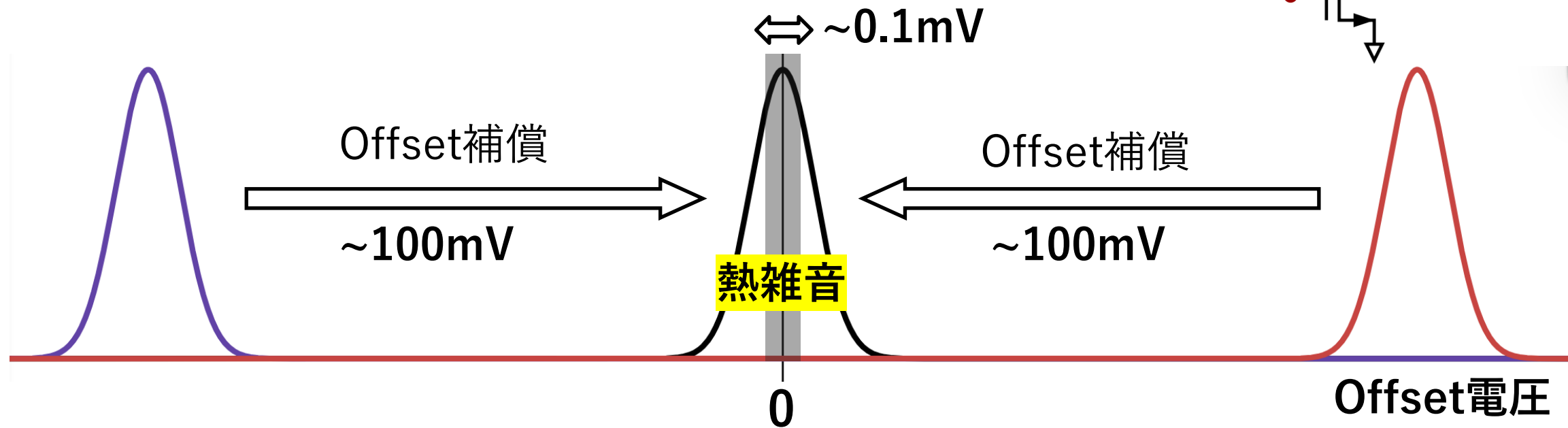
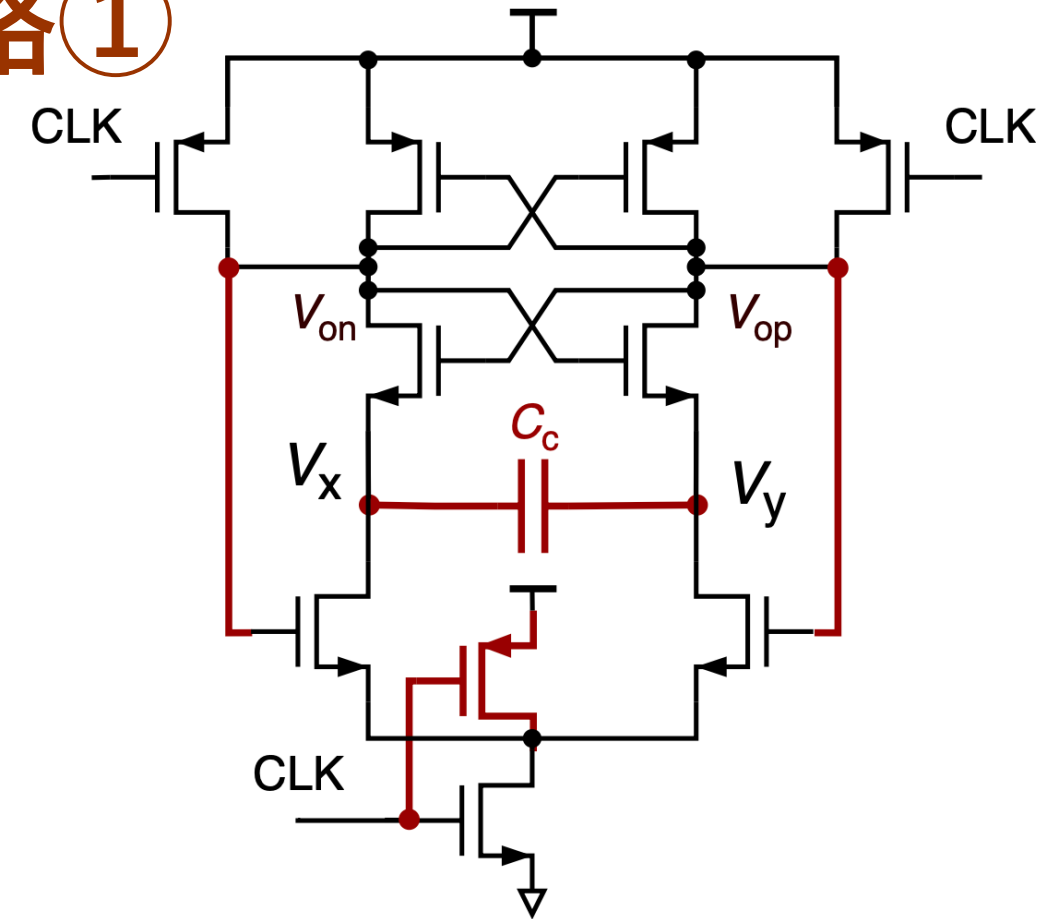
自己補正操作に問題あり

従来技術とその問題点

- 従来の高速な物理乱数発生回路は外部調整やキャリブレーションを必要とし、環境変動やプロセスばらつきに対する耐性や長期安定性に課題を有していた
 - **大きな消費電力**
 - **信頼性の問題**
- 自律補償機構を持つ従来の物理乱数生成回路の動作速度が遅い
 - **現代の通信に不十分**
- 従来のキャリブレーション技術と回路設計のコストが高い
- **低消費電力・高信頼性・高速・低コスト**の物理乱数生成回路がないため、物理乱数生成回路の応用が限定的

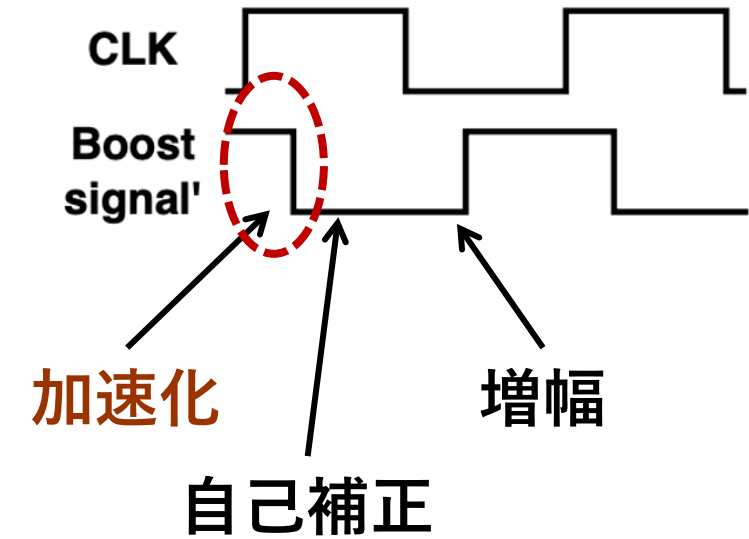
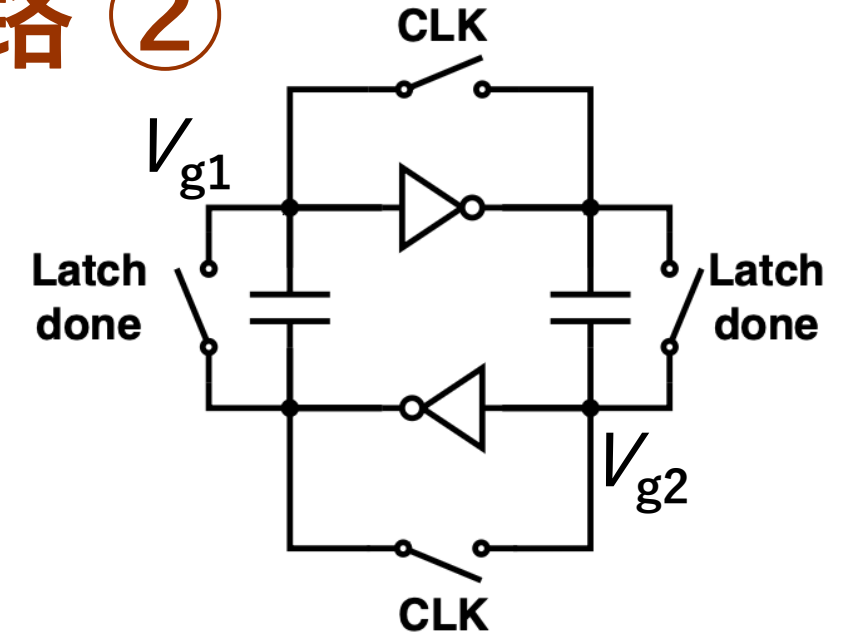
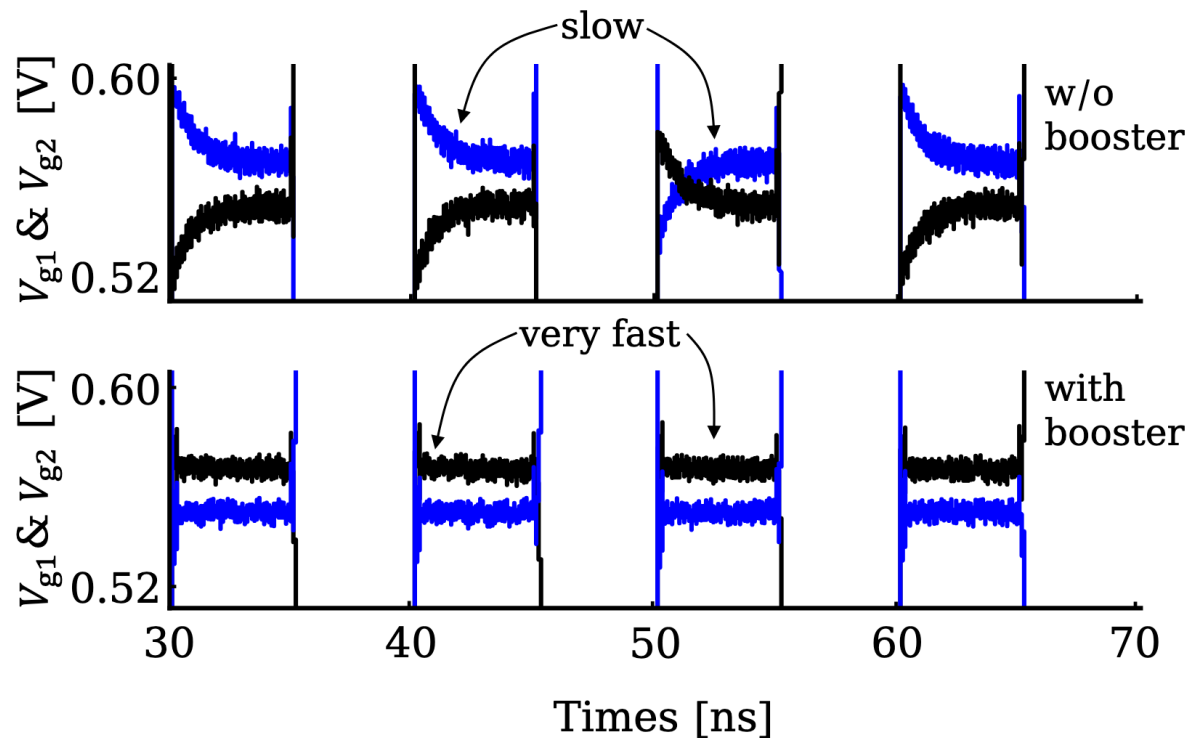
新技術に基づく回路①

- 電気ノイズを直接デジタル値に変換
 - 設計が容易 😊
 - 速い 😊
 - ばらつきの影響を自律補償 😊
- 動的アナログキャリブレーション
⇒ 小面積, 省エネルギー 😊



新技術に基づく回路 ②

- 電気ノイズを直接デジタル値に変換
 - 設計が容易 😊
 - 速い 😊
 - ばらつきの影響を相殺 😊
- 容量の小型化 ⇒ 小面積



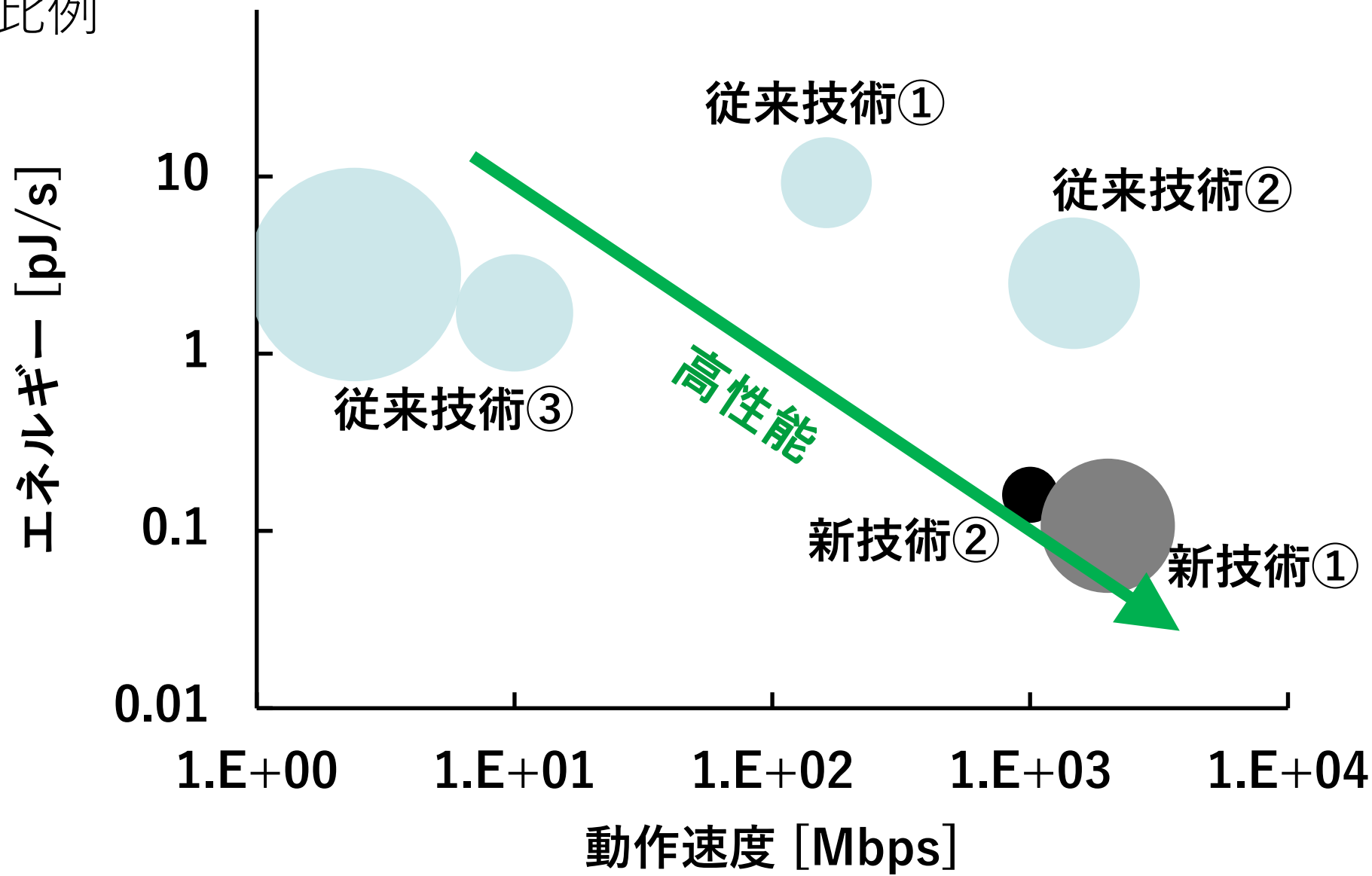
自己補正操作の問題を加速化操作により解決

RNGの性能比較

	PRNG	TRNG (物理乱数生成回路)				
	擬似乱数	リング発振 Synopsys社	Noise Intel社	Noise Samsung	Noise 新技術①	Noise 新技術②
乱数の質	×	△	○	◎	◎	◎
生成速度	○	△	◎	×	◎	○
回路面積	△	△	×	△	○	◎
消費電力	×	×	×	△	◎	○
設計容易さ	◎	○	×	○	◎	◎
製品例	電子機器	組み込みシステム	プロセッサ	IoTデバイス	すべて	すべて

性能比較

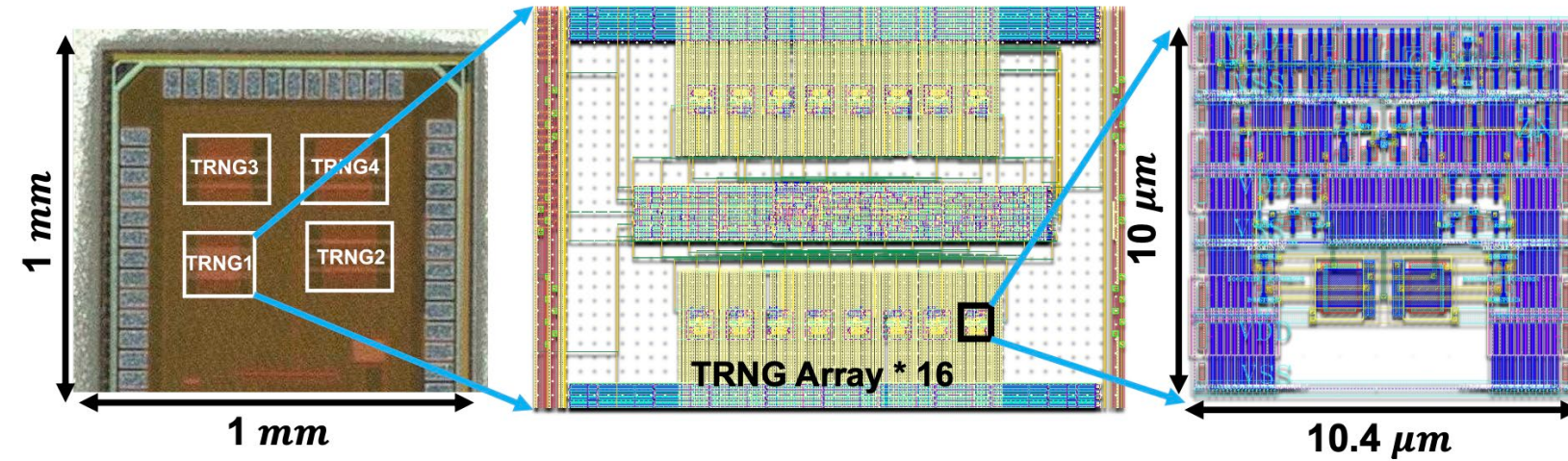
円は面積に比例



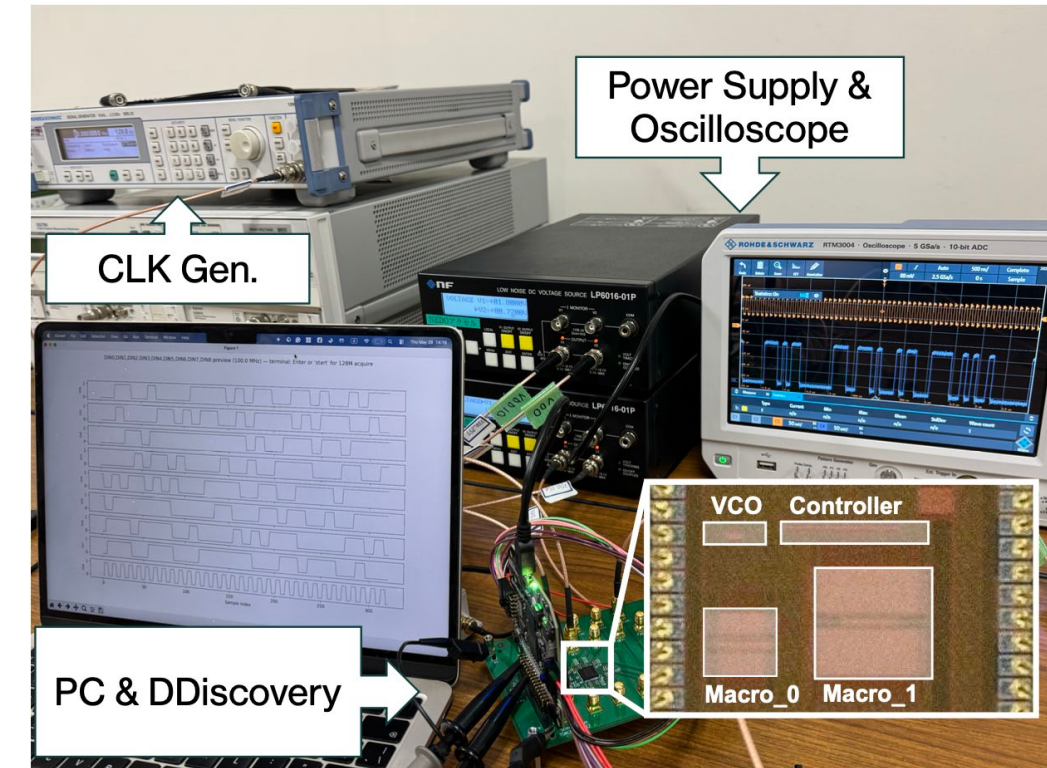
設計容易さ, プロセス可搬性, スケーラビリティなどにおいてさらなる優位性

TSMC 65nmチップにおける検証

ICレイアウト

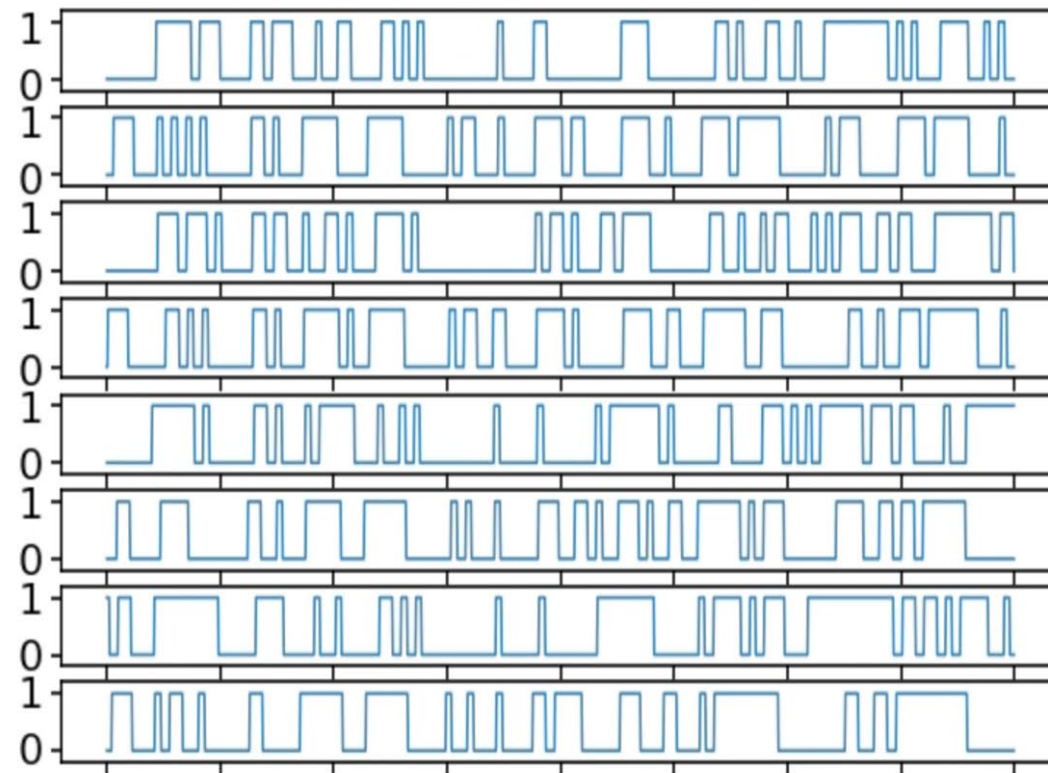


評価環境

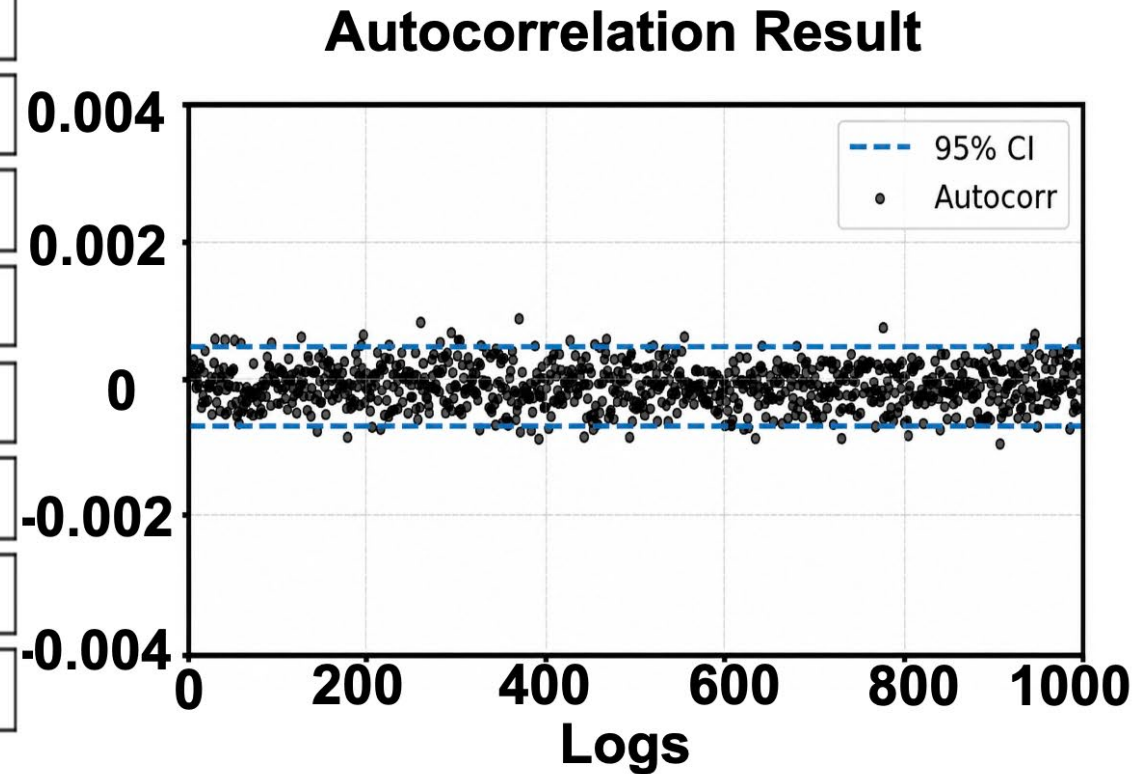


- TSMC 65nmプロセス
- 新技術①と新技術②のTRNG

新技術②の測定結果



Serial to Parallel Output Waveform



- 500 Mbpsでの検証完了
- NISTテストを合格
- 1 Gbps以上の動作能力
- 新技術①も160 Mbpsまで動作検証済み

新技術の特徴

💡 革新ポイント

- ✓ **熱雑音ベースで高強度な真の乱数を生成**
物理現象由来の予測不可能な乱数
- ✓ **自動補正により設計コストを大幅に削減し導入が容易に**
従来膨大な工数をかけていた補正作業を自動化
- ✓ **経年劣化への耐性**
長期運用においても自動でアップデートに対応し、品質を維持

新技術の従来技術との比較

既存技術の課題（セキュリティ vs 実用性）を一挙に解決

	実用性重視・脆弱 現状主流 (擬似乱数/発振器)	安全だが使いにくい 従来技術 (従来の熱雑音型)	Best of Both 本技術 (革新的な熱雑音型)
セキュリティ強度	△	◎	◎
設計コスト	◎	×	◎
導入期間・導入ハードル	短期 / 容易	長期 / 複雑で大量の補正が必要	短期 / 自動補正により容易
長期運用・保守	-	品質劣化 経年劣化に弱い	自動補正によりアップ デートにも対応可

想定される用途



- インターネットに繋がるすべての電子機器への応用可能
- 電力システムや銀行などの最重要な通信インフラのセキュリティ強化に特に有効

実用化に向けた課題

- 現在、65nmという先端プロセスで設計・検証済み
 - 500 Mbpsまで動作検証済み
 - 今後、より高い動作速度の実証を行う
- 今後、より微細なプロセスで実測を行い、低コストな開発を実証する
- 実用化できるほどの完成度はすでに有している

社会実装への道筋

時期	取り組む課題や明らかにしたい原理等	社会実装への取り組みについて
基礎研究	・ 回路の設計とレイアウトが完了	
現在	・ 実チップにおける動作検証	
今年後	・ 通信システムへの搭載 ・ IP化	デモンストレーション実施

企業への期待

- セキュアな低消費電力IoT製品への応用
- 電力システムや銀行システムなどの情報基盤への応用
- プロセッサなど半導体IC内に搭載
- スマホなど製品におけるカスタムICとして実装
- システム全体への統合について企業との共同研究を希望

企業への貢献、PRポイント

- 本技術はどのCMOSプロセスでも実現可能なため、現代システムアップデートや新規システム導入において、「セキュア保証」のブランドづくりに企業に貢献できる
- 本格導入にあたっての技術指導と共同開発が可能

本技術に関する知的財産権

- 発明の名称 : 物理乱数発生装置および物理乱数発生方法
- 出願番号 : 特願2025-042012/特願2025-163509
- 出願人 : 国立大学法人京都大学/東京科学大学
- 発明者 : イスラム エイケイエム マーフズル

産学連携の経歴

- 2025年-2026年 東京科学大学 スタートアップ支援事業
- 2025年-2030年 JST次世代エッジAI半導体研究開発事業

お問い合わせ先

東京科学大学 (Science Tokyo)

産学共創機構技術プロモーション室

T E L 03-5734-3817

e-mail consult@cim.isct.ac.jp