擬似乱数と真性乱数

- 擬似乱数
  - アルゴリズムに基づいた計算から生成
  - 必ず周期性を持つ
  - 初期値とアルゴリズムを与えられれば全ビットを再現可能
- 真性乱数
  - 物理的なランダム要因から生成(物理乱数)
  - 各ビットが互いに独立
  - 1/0 の発生確率が等しい
  - 予測不可能性を持つ

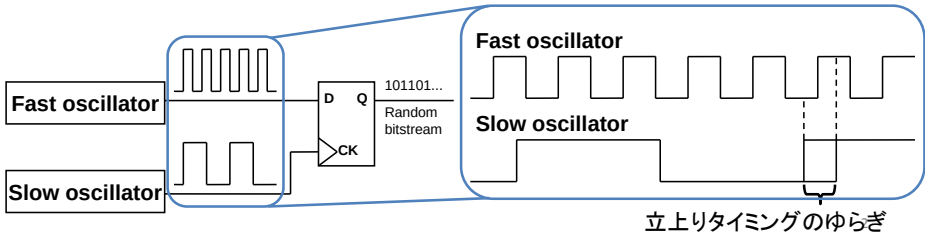
セキュリティ用途には不適当

秘密暗号鍵などに有用

オシレータサンプリング方式
TRNG(True random number generator)

- 真性乱数生成回路の一方式(ランダム要因:内部雑音)
- 高速・低速2つのオシレータを使用
- 高速の発振信号をデータ、低速の発振信号をクロックとしてサンプリング
- クロックの周期ゆらぎからランダム性を獲得

- 実装が容易
- 高品質乱数を得ることが困難
  ⇒ 後処理が必要



目的

- 高品質乱数を生成するオシレータサンプリング方式TRNGの実現
  - オシレータサンプリング方式の乱数品質評価
    - 品質改善に有効な動作パラメータの確認
    - 外部雑音への耐性の評価
  - ゆらぎ増幅回路の提案
    - 低コストな乱数品質改善

今後の研究課題

- オシレータサンプリング方式TRNG
  - ランダム要因:回路内雑音(熱雑音など)
  - 温度の低下やデバイスの経年変化
    ⇒ 乱数品質が劣化する可能性

- 環境変動や経年変化に対する耐性
  - 環境変動、乱数品質の劣化を検知
  - 自律的に動作パラメータを調節
    ⇒ 悪環境においても高品質の乱数を生成