乱数品質を保証したオンチップハードウェア乱数発生器の開発

橋本昌宜
大阪大学情報科学研究科
hasimoto@ist.osaka-u.ac.jp

セキュリティにおける乱数

- 暗号・認証システム
  - 第三者から予測不可能な乱数が必要

    例）秘密鍵・公開鍵の生成、Diffie-Hellman鍵交換、チャレンジアンドレスポンス認証
- 真性乱数生成器 (True random number generator)
  - 物理的なランダム要因から乱数を生成
    - 計算による予測が不可能（⇔疑似乱数）
  - 要求される品質
    - 高い統計的ランダム性
    - セキュリティ用途では環境変動への耐性も必要

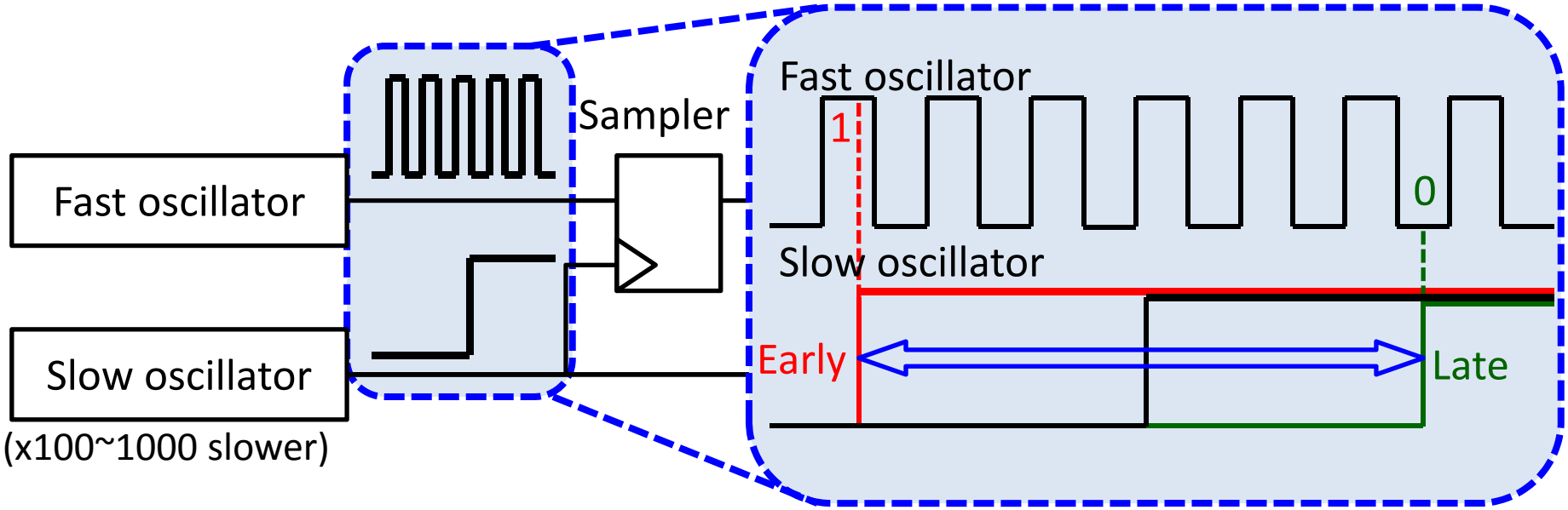
開発した乱数生成回路の特徴

- 容易なオンチップ搭載
  - 専用デバイスを必要としない簡易なデジタル回路
- 乱数品質の保証
  - 乱数出力を常に監視し、回路の自己調整により品質低下を防止
- 柔軟なスループット
  - 乱数品質とのトレードオフにより柔軟なスループットを実現
- 耐タンパー性
  - 意図的な電源ゆらぎ攻撃に対する耐性を実現

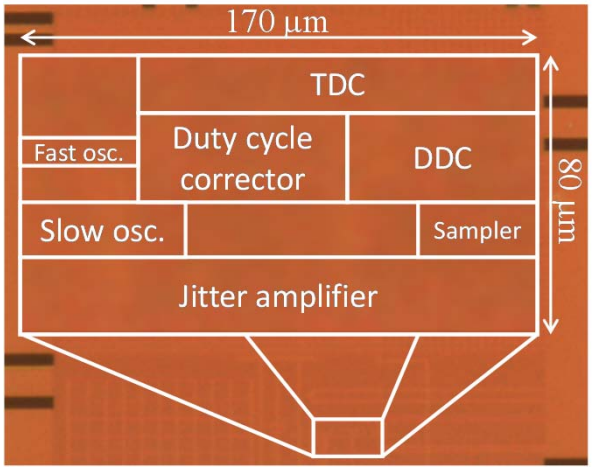
オシレータベース真性乱数生成回路

- オシレータのランダムな周期ゆらぎを利用
- 長所: 実装が容易、外乱に一定の耐性
- 短所: 高品質乱数を得ることが困難
  - 原因）低速-周期ゆらぎの不足
    デューティ比の崩れ

ゆらぎ増幅回路で克服
自己調整機構で克服



開発した乱数生成器の性能



- 65nmプロセスで試作
- NIST乱数テストに合格する乱数生成器で最小面積実装を達成

	Bucci2003[11]	Bucci2008[3]	Pareschi2010[12]	Srinivasan2010[2]	This work
Principal	Direct amp.	Oscillator-based	Chaos-based	Metastable-based	Oscillator-based
Technology	180 nm	90 nm	180 nm	45 nm	65 nm
Area	25,000 μm^2	13,000 μm^2	126,000 μm^2	4,004 μm^2	6,670 μm^2
Area normalized to 45nm	1,563 μm^2	3,250 μm^2	7,875 μm^2	4,004 μm^2	3,335 μm^2
Throughput	40 Mbps	1.74 Mbps	80 Mbps	2.4 Gbps	7.3 Mbps
Randomness Assessment	FIPS140-1 Knuth	AIS31 Entropy eval.	NIST SP800-22	NIST SP800-22 Entropy eval. Autocorrelation eval. Run length eval.	NIST SP800-22 DIEHARD
Post processing	XOR	LSFR	-	-	-