Novel TRNG Verification with a High-Performance Simulation Methodology

Presentation by
Ting-Yen Chiang, Sr. Analog Design Engineer**, Microsoft**
Shravan Ramesh, Application Engineer, **Siemens**
Lih-Jen Hou, Product Manager, **Siemens**

SIEMENS Microsoft

62 THE CHIPS TO SYSTEMS CONFERENCE

SPONSORED BY CEDA® IEEE Council on Electronic Design Automation SIGDA acm

Ting-Yen Chiang

Sr. Analog Design Engineer

Microsoft

Lih-Jen Hou

Product Manager

Siemens EDA

Shravan Ramesh

Application Engineer

Siemens EDA

In This Presentation

*We will explore the complex verification challenges associated with these two TRNGs and highlight how the collaboration between **Microsoft** and **Siemens EDA** has enabled a breakthrough simulation approach.*

*We will demonstrate a new simulation workflow using the **Siemens Solido Simulation Suite** that dramatically enhances both accuracy and efficiency in TRNG verification, while maintaining the highest standards of randomness validation.*

Motivation

The growing importance of TRNGs in encryption for data security

- True Random Number Generators (TRNGs) use natural random phenomena like noise to generate truly random numbers for hardware

- Unpredictability of noise makes TRNG outputs nearly impossible to predict, enhancing security in data encryption applications

Motivation

Addressing verification challenges for True Random Number Generators (TRNGs)

Challenges in verifying modern TRNGs

- Verification challenge: Ensuring true randomness during the design flow is difficult, requiring efficient extraction and simulation of TRNG characteristics
- Time-consuming simulations: Verifying TRNGs with time-domain simulations can take over a year, making the design flow impractical
- System complexity: Various types of oscillators in TRNGs make it difficult to select a verification method

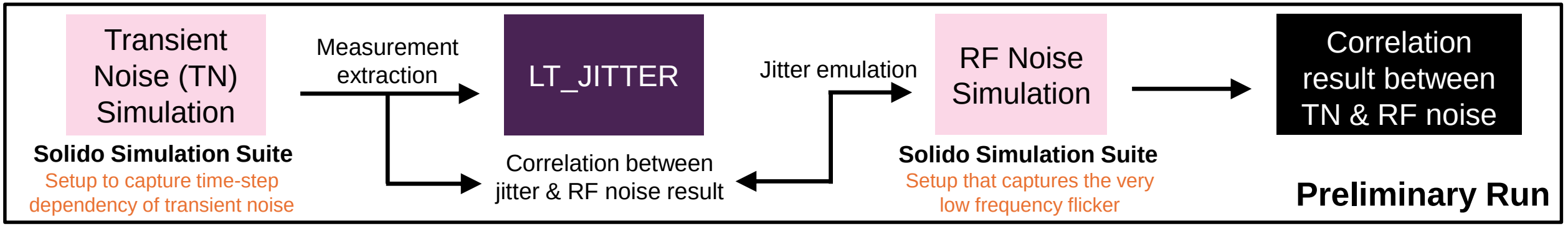
A revolutionary simulation flow significantly boosts the efficiency of TRNG verification

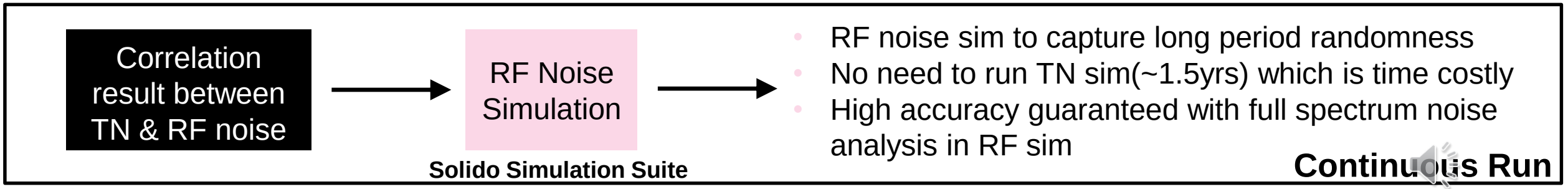
Main Idea

Achieving an efficient verification flow by integrating diverse simulation tools

Verifying Free-Running Ring-Oscillator (RO) TRNGs

- TN sim challenge: Low sampling rate leads to long simulation time (~1.5 yrs) to measure long-term(LT) jitter
- RF noise sim challenge: Sensitive to impacts from very low frequency flicker noise
- Optimized methodology needed to overcome these challenges



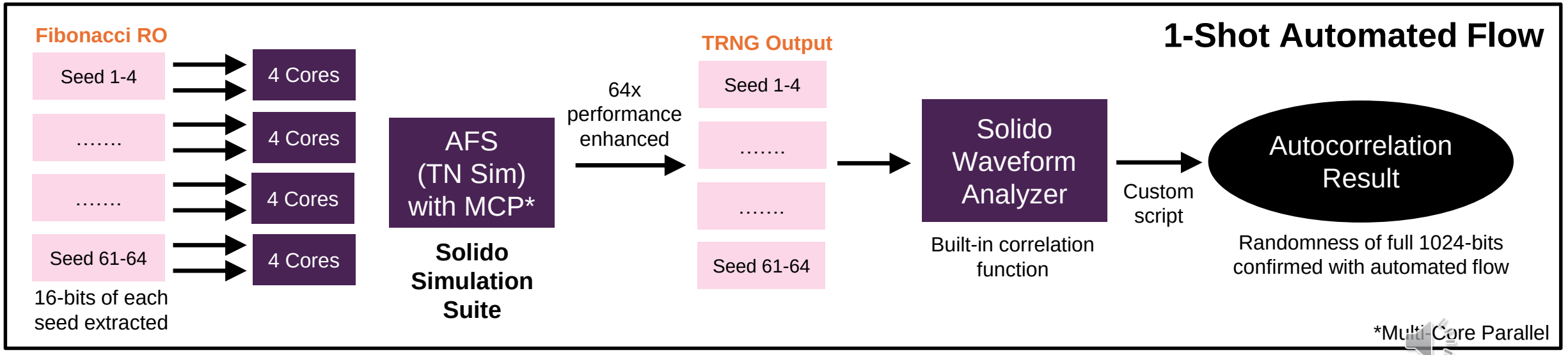


Main Idea

How to realize the verification flow through integration

Verifying Fibonacci-Galois Ring-Oscillator TRNGs

- Challenges:
  - Fibonacci-Galois RO has no steady-state - thus RF analyses cannot be run
  - TN simulation for this RO requires 1024-bit results for initial sign-off, but 30 hours required for only 16 bits
- Optimized methodology needed to overcome these challenges

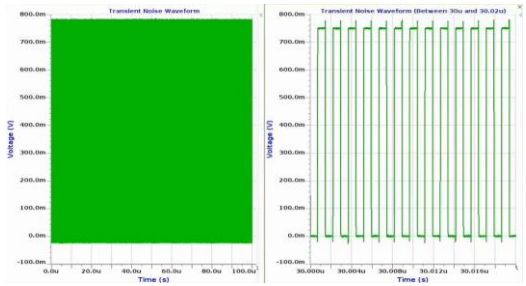


Evidence

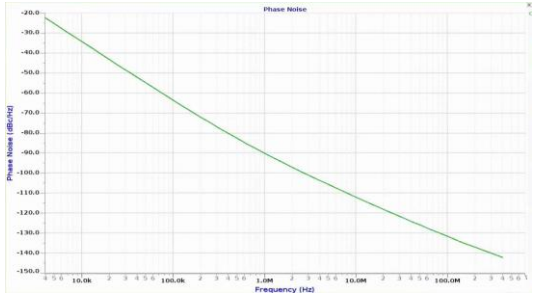
How the new simulation flow was evaluated: **Free-Running Ring-Oscillator (RO) TRNGs**

Solido Simulation Suite

TN Simulation



RF Noise Simulation



- Run initial sim for TN and RF Noise simulations

Solido Waveform Analyzer

- Allow LT_Jitter to be extracted from Solido Waveform Analyzer
- This function is embedded in Solido Waveform Analyzer
- Applicable for RF Noise and TN

Solido Waveform Analyzer

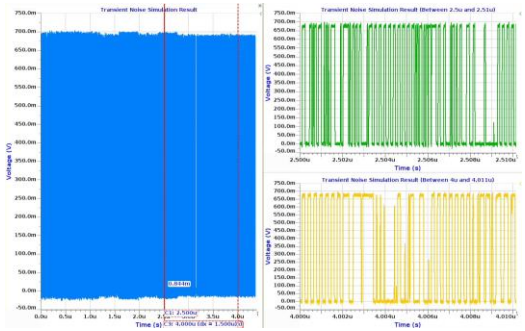
- Check the correlation of the noise value from both TN sim and RF noise
- Once we confirmed the noise in the certain time, RF noise sim can be used for longer simulation
- Overall TAT reduced by 300x with using RF sim only

Evidence

How the new simulation flow was evaluated: **Fibonacci-Galois Ring-Oscillator TRNGs**

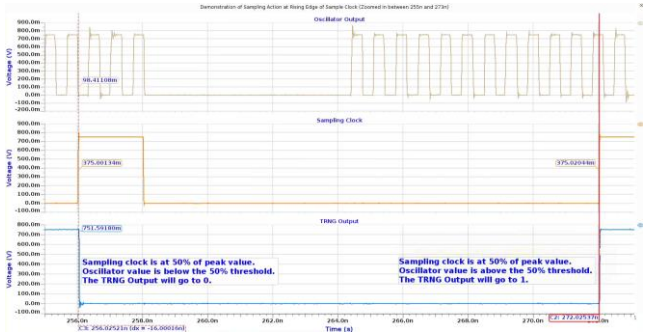
Solido Simulation Suite

Fibonacci RO TN



- Run separate 16-bits data with 64 seeds

Solido Waveform Analyzer

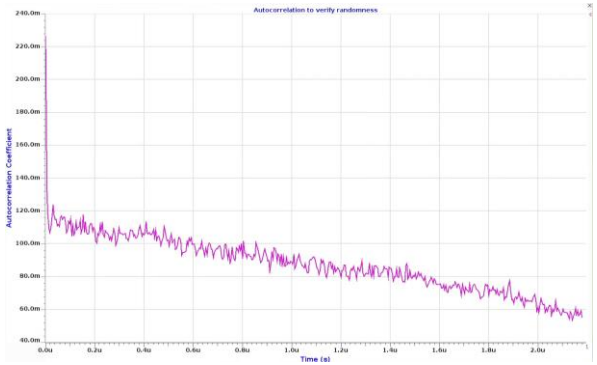


- Verify sampling behavior for 1 edge

Solido Waveform Analyzer

- Create custom script to automate sampling behavior and determine bias

Final Correlation with Solido Waveform Analyzer

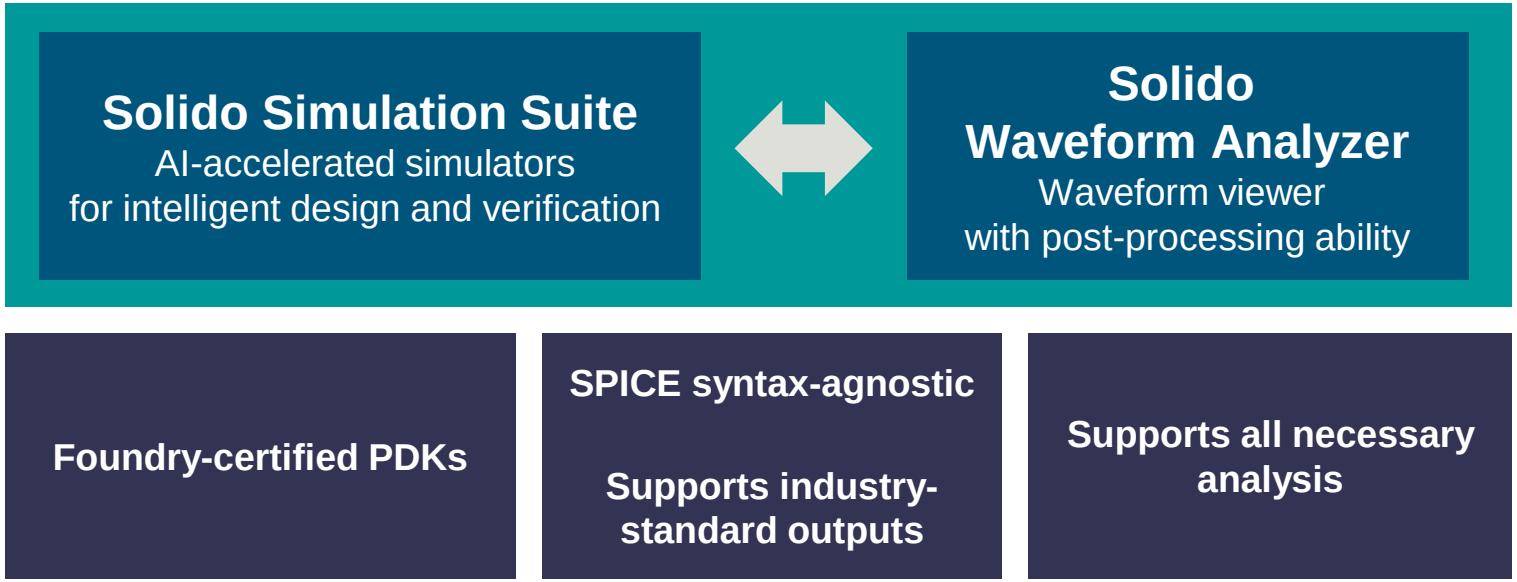


- Embedded function in Solido Waveform Analyzer
- Randomness of full 1024-bits confirmed with automated flow

Evidence

How Siemens EDA's solution achieve the efficient design flow for TRNG

Integrated of SPICE simulation and embedded post-processing



- **Solido Simulation Suite** delivers excellent accuracy for TN simulations, enabling precise RF correlation and accelerating TRNG verification
- **Solido Simulation Suite** offers Multi-Core Parallel (MCP) technology, enabling efficient parallelization of seeds simulations across multiple cores, thereby enhancing overall efficiency
- **Solido Waveform Analyzer** offers embedded functions for capturing long-term(LT) jitter, customizable scripting for automation, and easy post-processing capabilities, providing users with flexibility and usability

Summary

- Data security is crucial in the digital world, and encryption protects sensitive information - TRNGs generate unpredictable random numbers to enhance security

- Microsoft is dedicated to studying various combinations of TRNGs and managing the associated simulation challenges
  - **Verification of Free-Running RO TRNGs:** TN simulation is too slow(~1.5yrs), and RF noise is sensitive
  - **Verification of Fibonacci-Galois RO TRNGs:** RF noise simulation is impractical due to unstable frequencies and capturing randomness from multiple oscillators

- Microsoft is collaborating with Siemens EDA to develop a new simulation flow to overcome these challenges
  - **Free-Running RO TRNG:** By utilizing the Solido Simulation Suite to accurately correlate TN and RF noise, and performing RF noise simulations to achieve equivalent long-period randomness with a reasonable turnaround time, we have enhanced simulation performance by **300x**.
  - **Fibonacci-Galois RO TRNG:** Using Solido Simulation Suite to extract 16-bit data from each of the 64 different noise seeds from a single oscillator and Solido Waveform Analyzer for an automated flow to efficiently enhance simulation performance by **64x**