TÜBİTAK

A New Evaluation Method for RNG

Ülkühan Güler

National Research Institute of Electronics and Cryptology

TURKEY

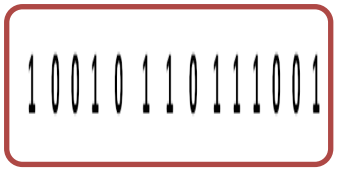
Outline

- Introduction
- Jitter Analysis Tools
- Characteristics and Causes of Each Jitter Components
- RNG Evaluation and Attack Scenario
- Conclusion

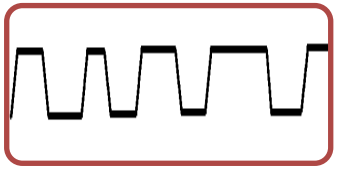
Aim

- To propose a rapid RNG evaluation method from a practical point of view that does not rely on complex math.

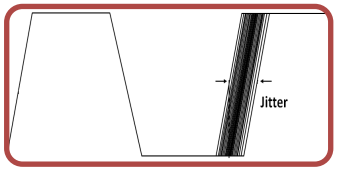
Introduction



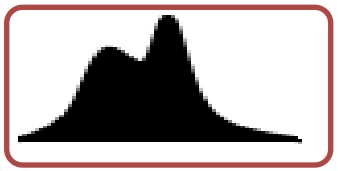
Conventional RNG evaluation methods are complex and so many statistical process are held on binary data



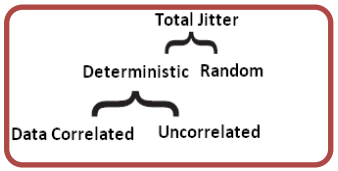
On the other hand, actually, binary data constitute from signal waveform



Jitter is the source of randomness in the binary data



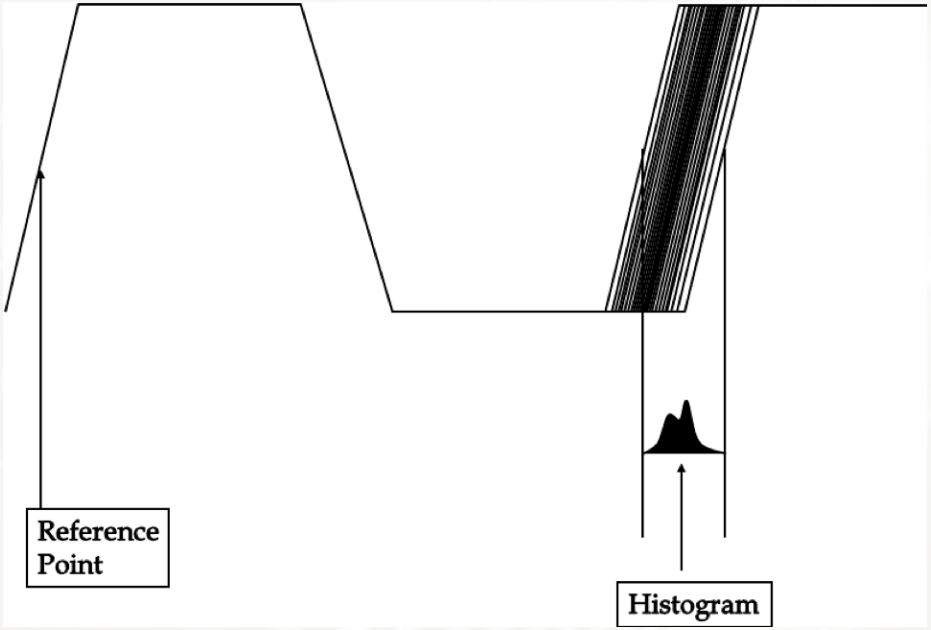
Jitter may have both random and deterministic components



By analyzing jitter components, we can determine the dominant component in the waveform

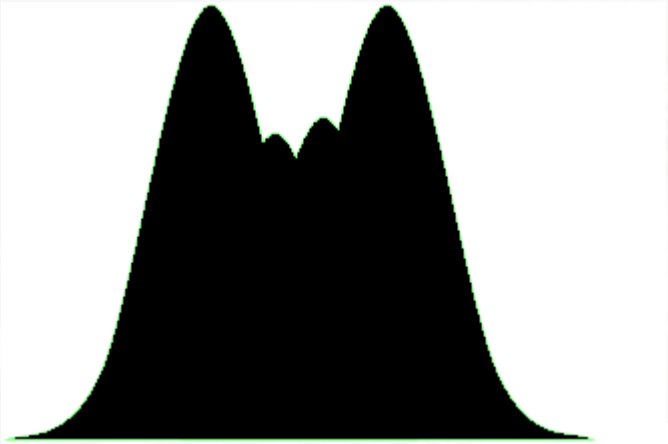
What is Jitter?

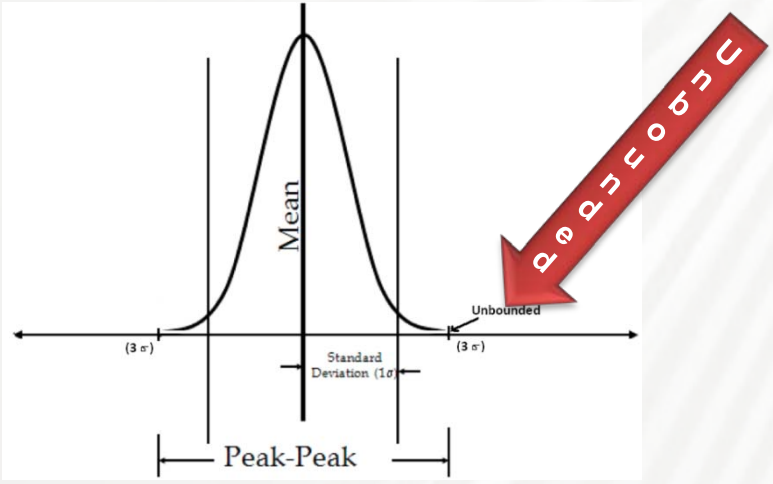
- Jitter is the timing variations in the signal

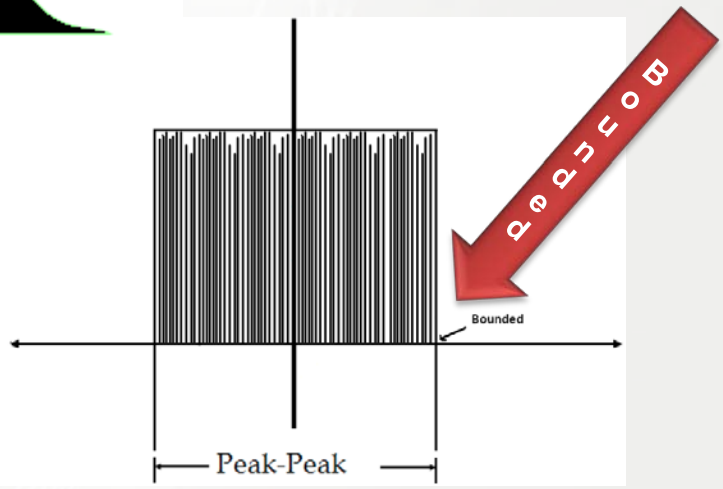


Jitter Analysis

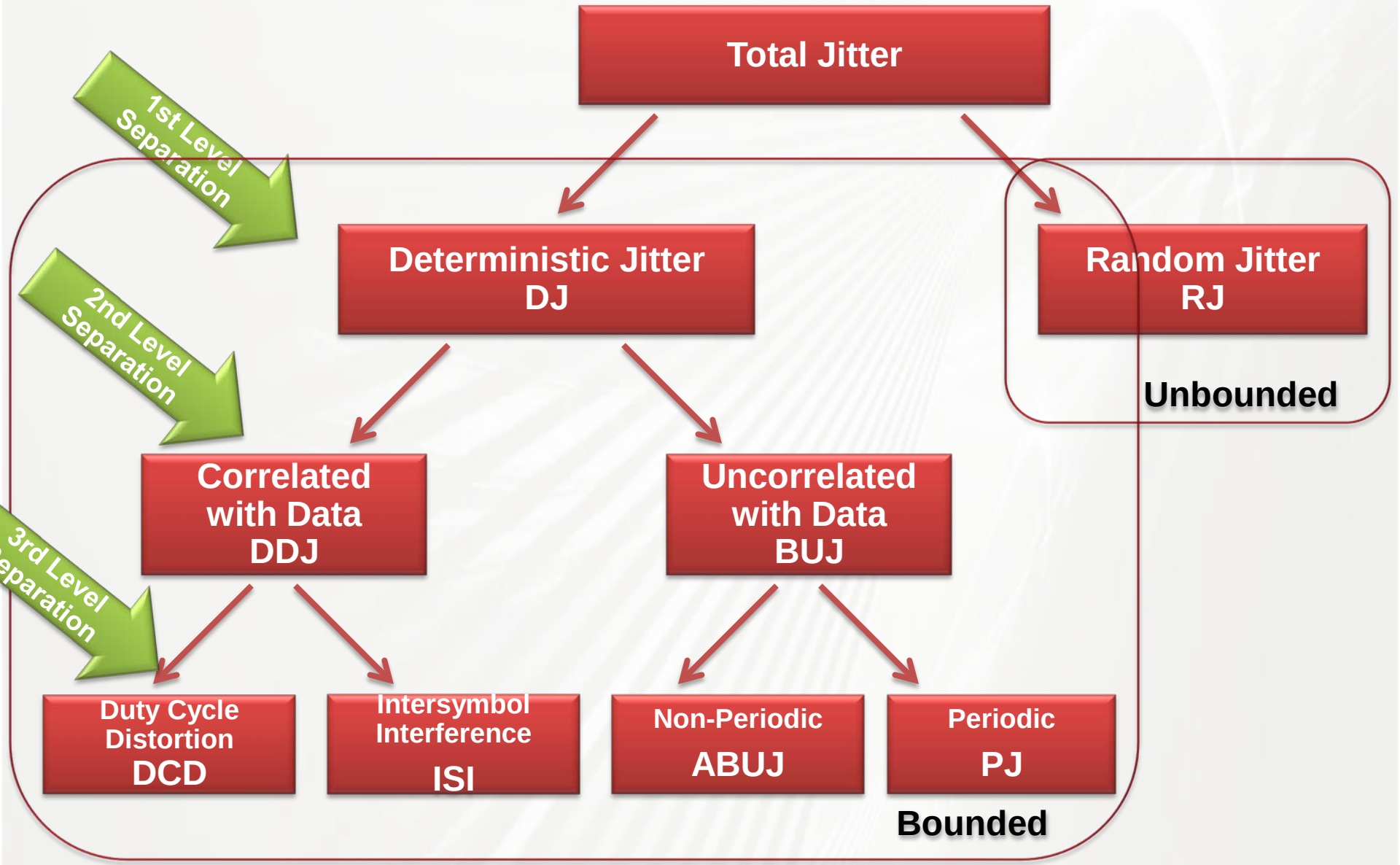
- Jitter has random and deterministic components and can be analyzed by histograming tools







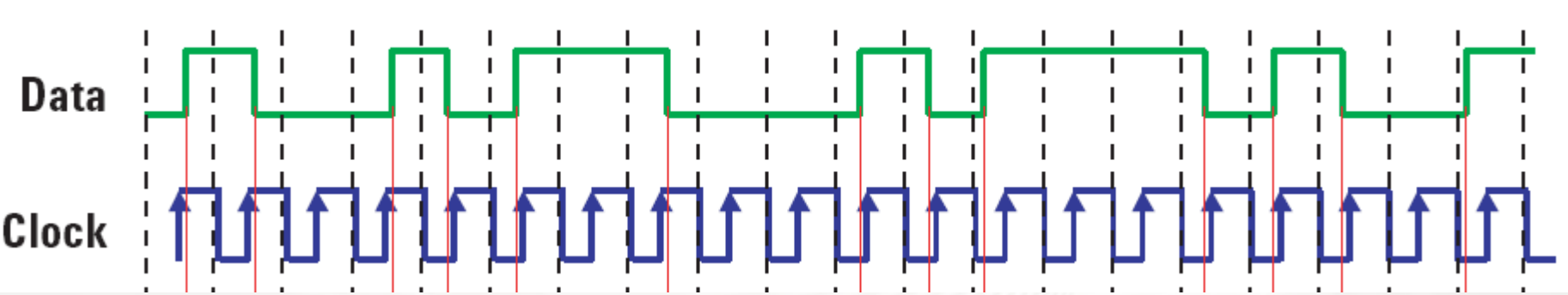
Jitter Components

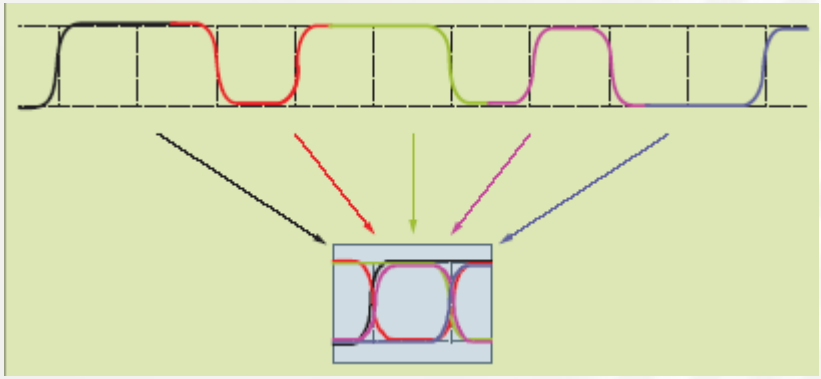


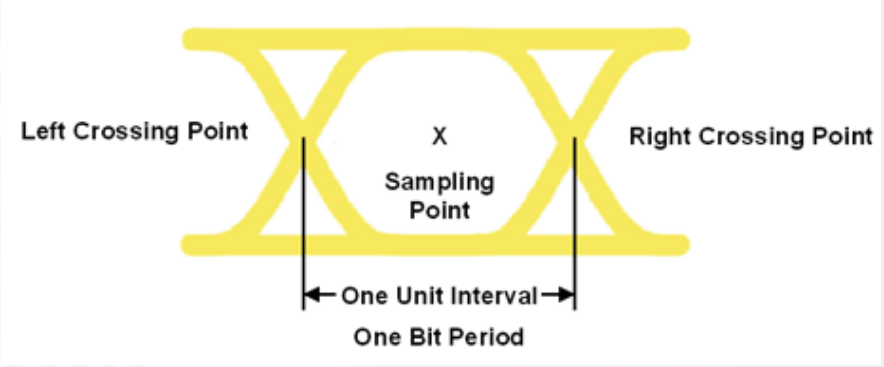
Outline

- Introduction
- Jitter Analysis Tools
- Characteristics and Causes of Each Jitter Components
- RNG Evaluation and Attack Scenario
- Conclusion

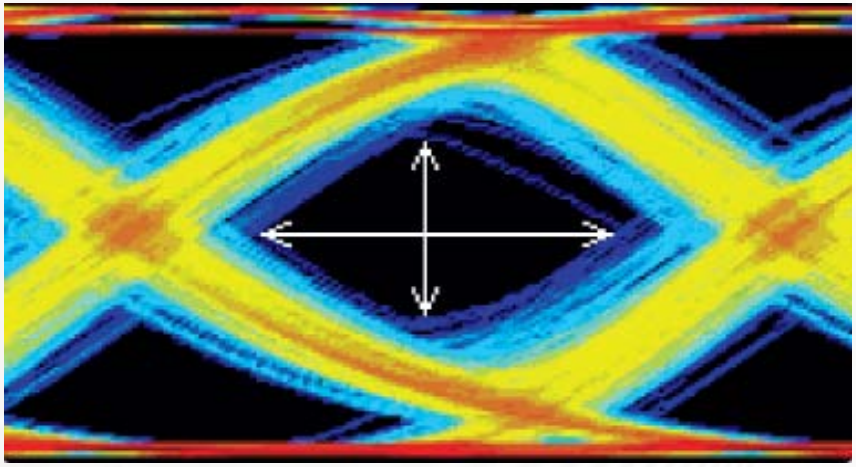
Eye Diagram

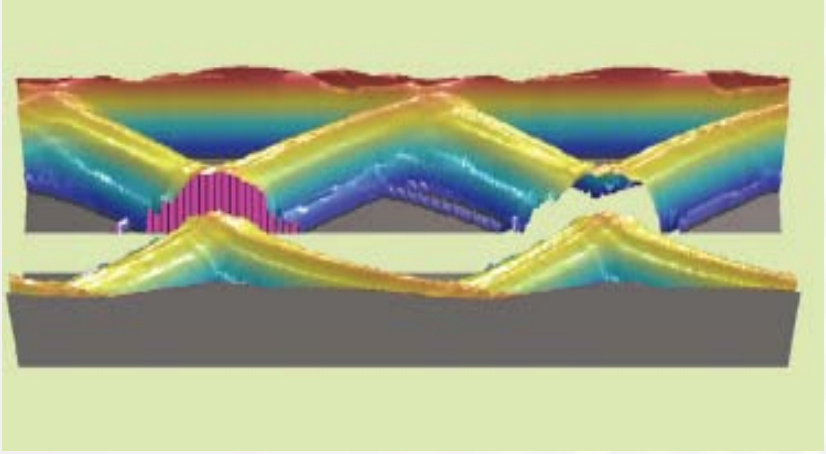

Data
Clock

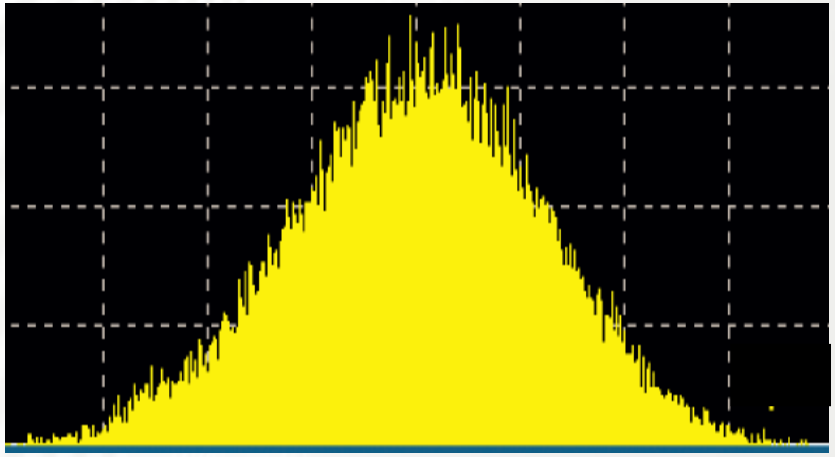



Left Crossing Point
X
Sampling Point
Right Crossing Point
One Unit Interval
One Bit Period

Histogram

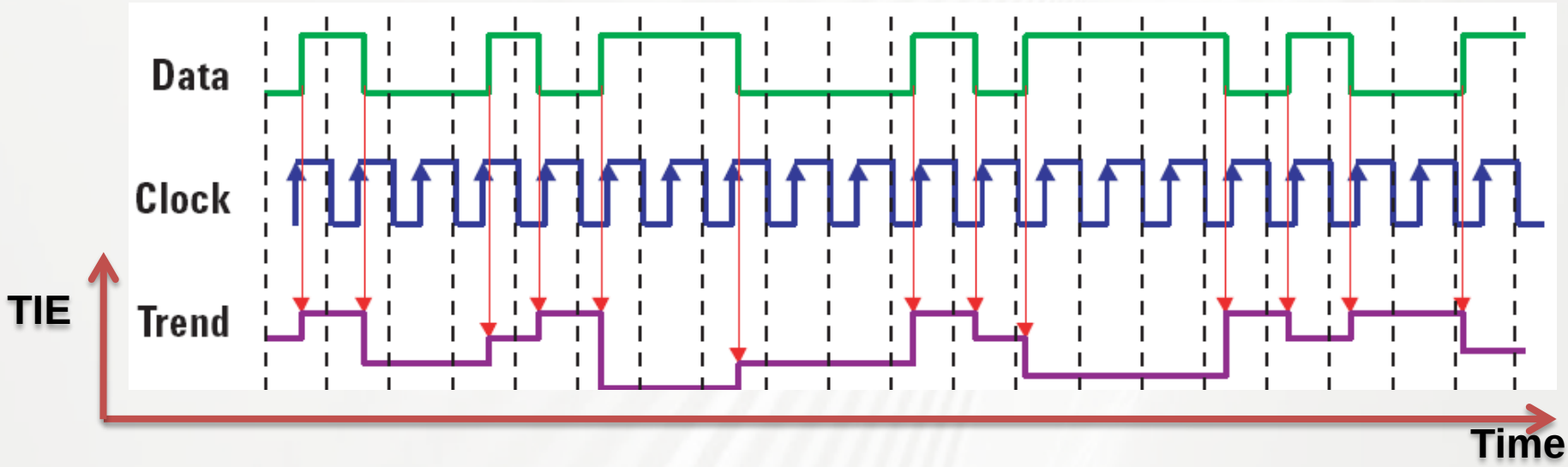






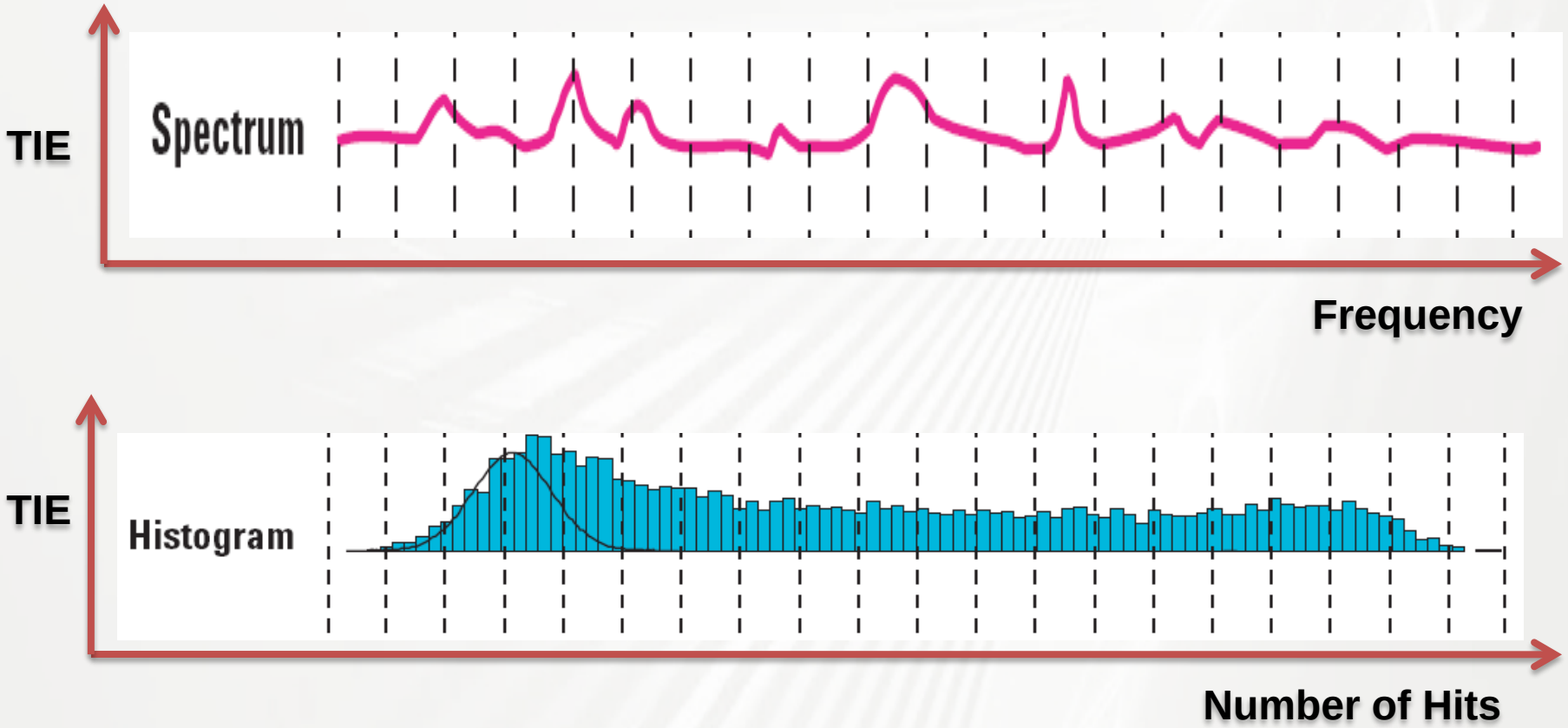
Time Interval Error (TIE)

- Eye Diagram along with histogram gives an intuitive feel about the type of jitter
- For deep insight and identification of jitter components, time-correlate measurement tools are used



- The timing error between the edges of ideal clock and data is Time Interval Error (TIE)

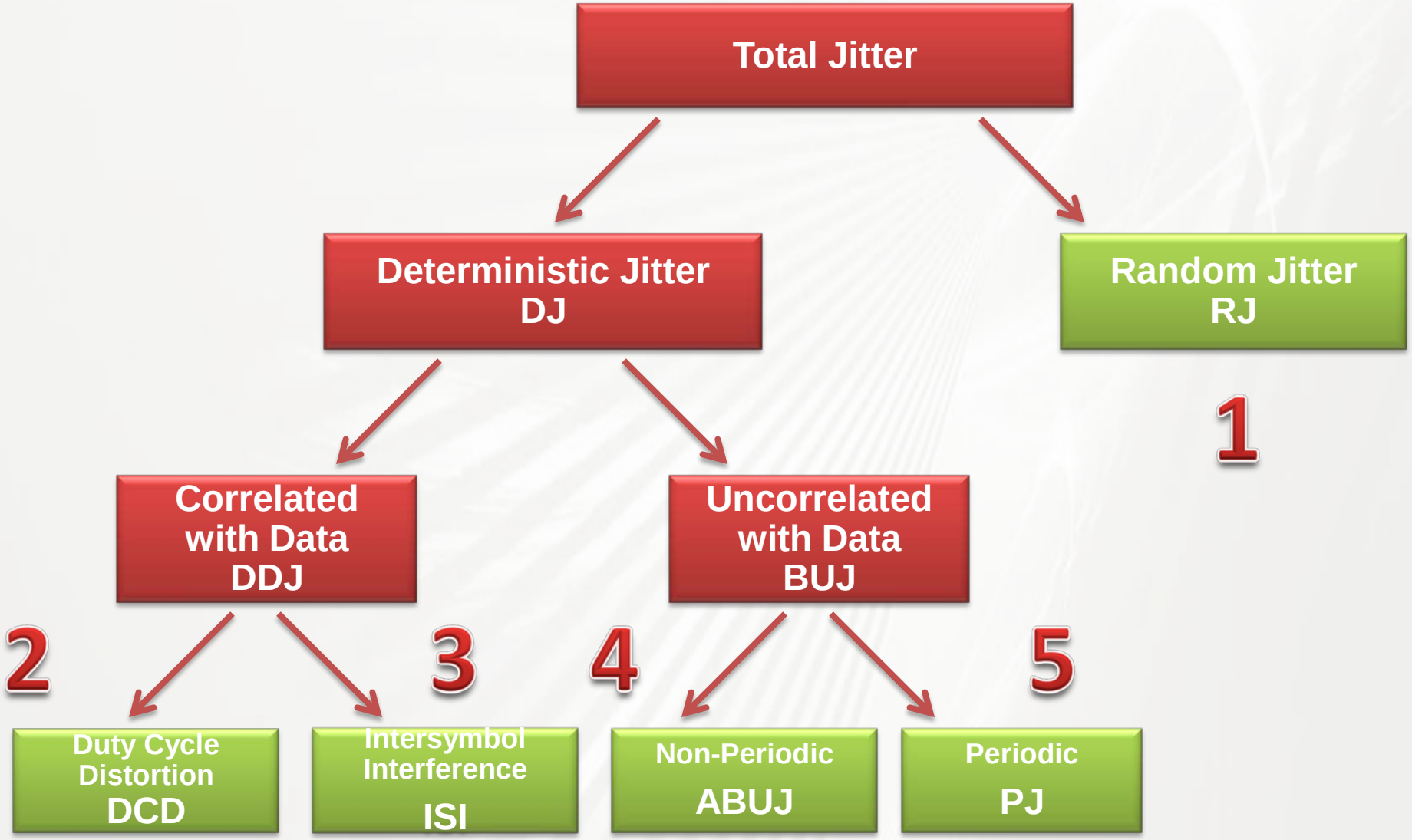
Spectrum and TIE Histogram



Outline

- Introduction
- Jitter Analysis Tools
- Characteristics and Causes of Each Jitter Components
- RNG Evaluation and Attack Scenario
- Conclusion

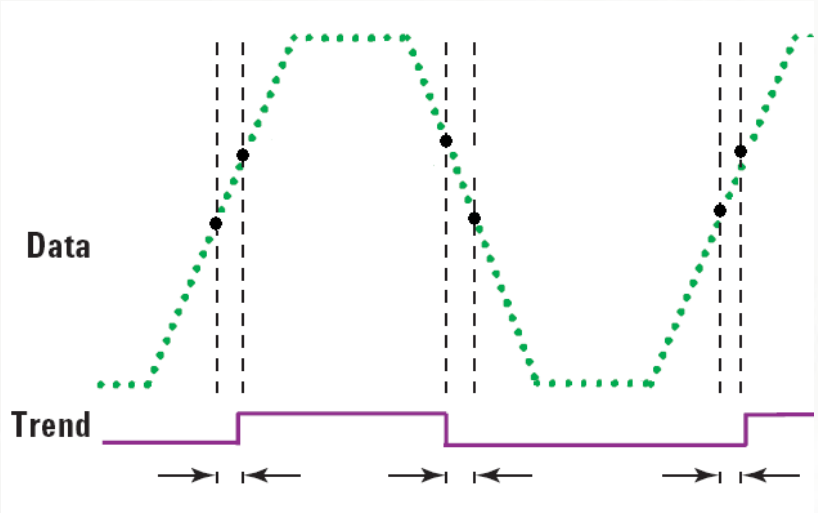
Jitter Components



Random Jitter (RJ) — 1

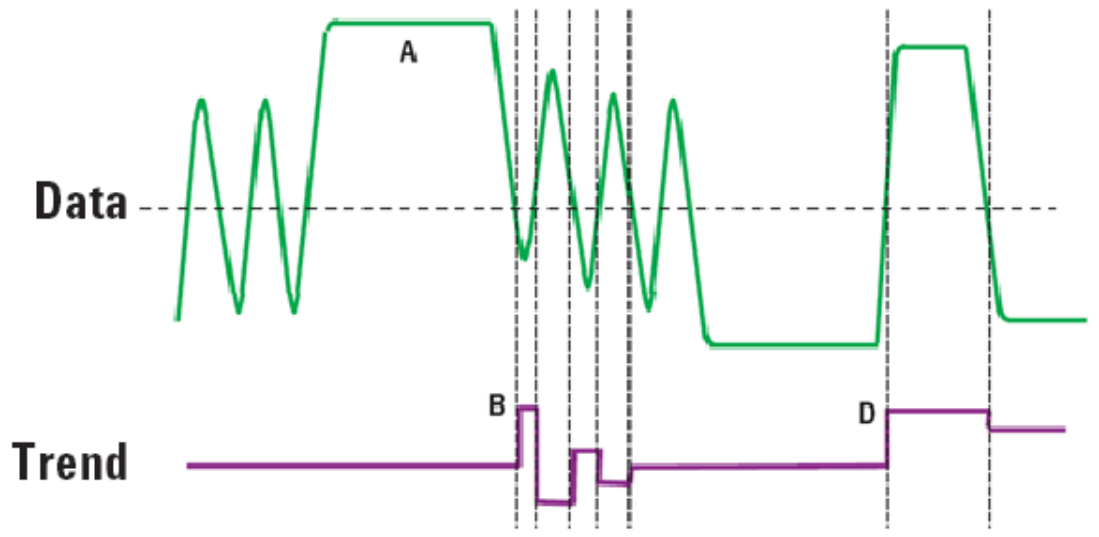
- Is good for RNG
- Random noise transforms to random timing jitter in the waveform, which actually is the entropy source of RNG
- Has a Gaussian Distribution
- Is unbounded therefore unlimited in terms of peak-to-peak values
- Measured with an RMS value (1σ)
- Caused by thermal, shot and 1/f noises in semiconductor elements

Duty Cycle Distortion (DCD) — 2



- Two primary causes
  - Threshold level of transmitter
  - Asymmetry in rising and falling edges of the signal

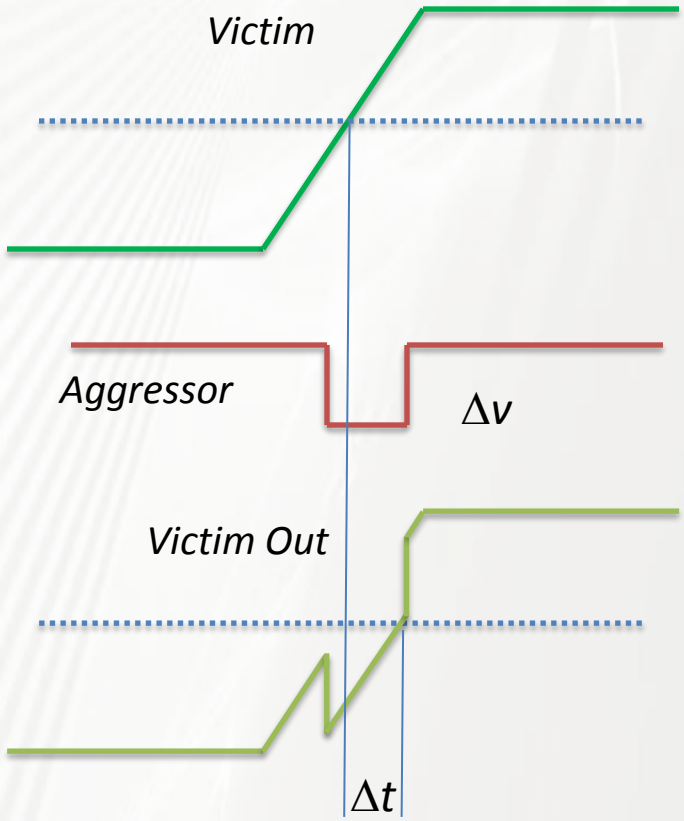
Intersymbol Interference (ISI) — 3



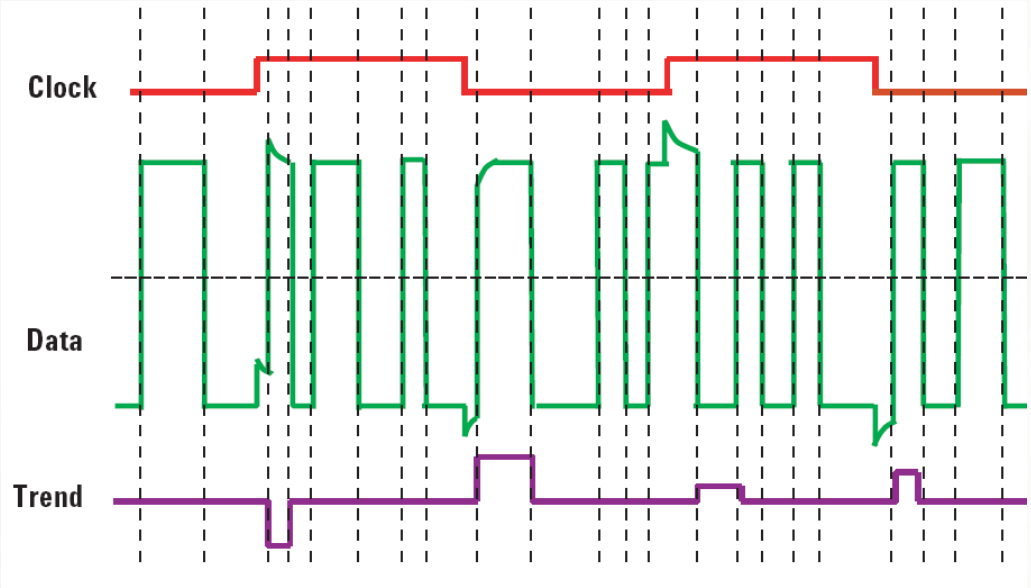
- Two primary causes
  - Bandwidth limitation problem of the transmitter or physical media
  - Reflection due to impedance termination mismatches and physical media discontinuities

Non-periodic Jitter (ABUJ) — 4

- Also called as Aperiodic Bounded Uncorrelated Jitter (ABUJ)
- Two primary causes
  - Crosstalk
  - Ground Bounce



Periodic Jitter (PJ) — 5



- Two primary causes
  - Cross-coupling (coupled to clock signals)
  - EMI (Power supply switching, magnetic influences)

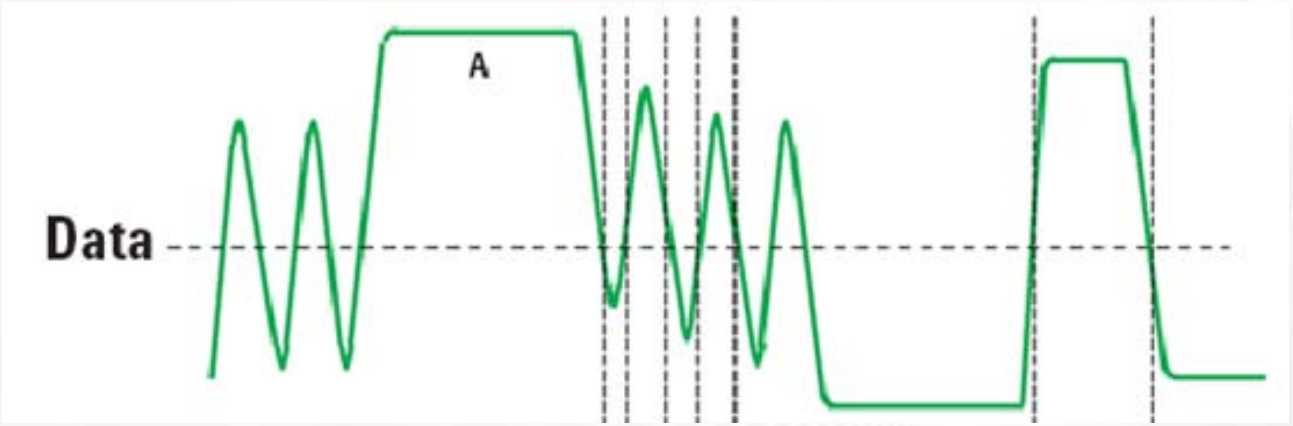
Outline

- Introduction
- Jitter Analysis Tools
- Characteristics and Causes of Each Jitter Components
- RNG Evaluation and Attack Scenario
- Conclusion

RNG Evaluation

1- Random Jitter	• Thermal, Shot, 1/f
2- DutyCyle Distortion (DCD)	• Threshold of transmitter • Asymmetry in rise and fall time
3- InterSymbol Interference (ISI)	• Bandwidth limitations • Reflection due to impedance mismatches
4- NonPeriodic Jitter (ABUJ)	• Crosstalk • Ground bounce
5- Periodic Jitter (PJ)	• Clock correlation • Switching effect of power supply

Attack Scenario - Predicting Key



- If there is ISI in the waveform, certain patterns follow some certain bits
- Attacker can predict the key with patterns

Attack Scenario - Modulating Clock or Injecting Patterns

- If the RNG seems weak in terms of periodic jitter component
  - Modulating clock
  - Injecting patterns over power supply

attacks can be applied to RNG

Outline

- Introduction
- Jitter Analysis Tools
- Characteristics and Causes of Each Jitter Components
- RNG Evaluation and Attack Scenario
- Conclusion

Conclusion

- A Practical RNG Evaluation Method is proposed for the use of practical evaluations in the design stage before complex mathematical evaluation methods are applied to RNG during evaluation stage.

- RNG attack scenarios can be developed after the interpretation of analysis results.

Thank you for your attention!