Random Number Generation Using Amplified Spontaneous Emission in a Fiber Amplifier

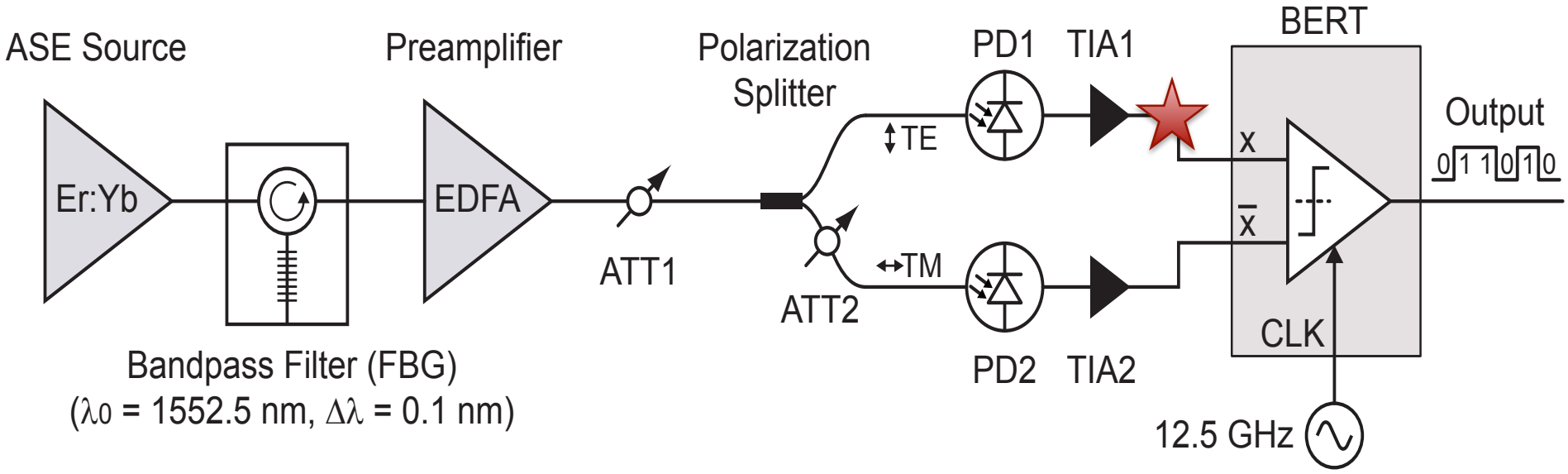
Julia C. Salevan, Caitlin R. S. Williams,
Xiaowen Li, Thomas E. Murphy, Rajarshi Roy

TREND Fair 2010

Motivation

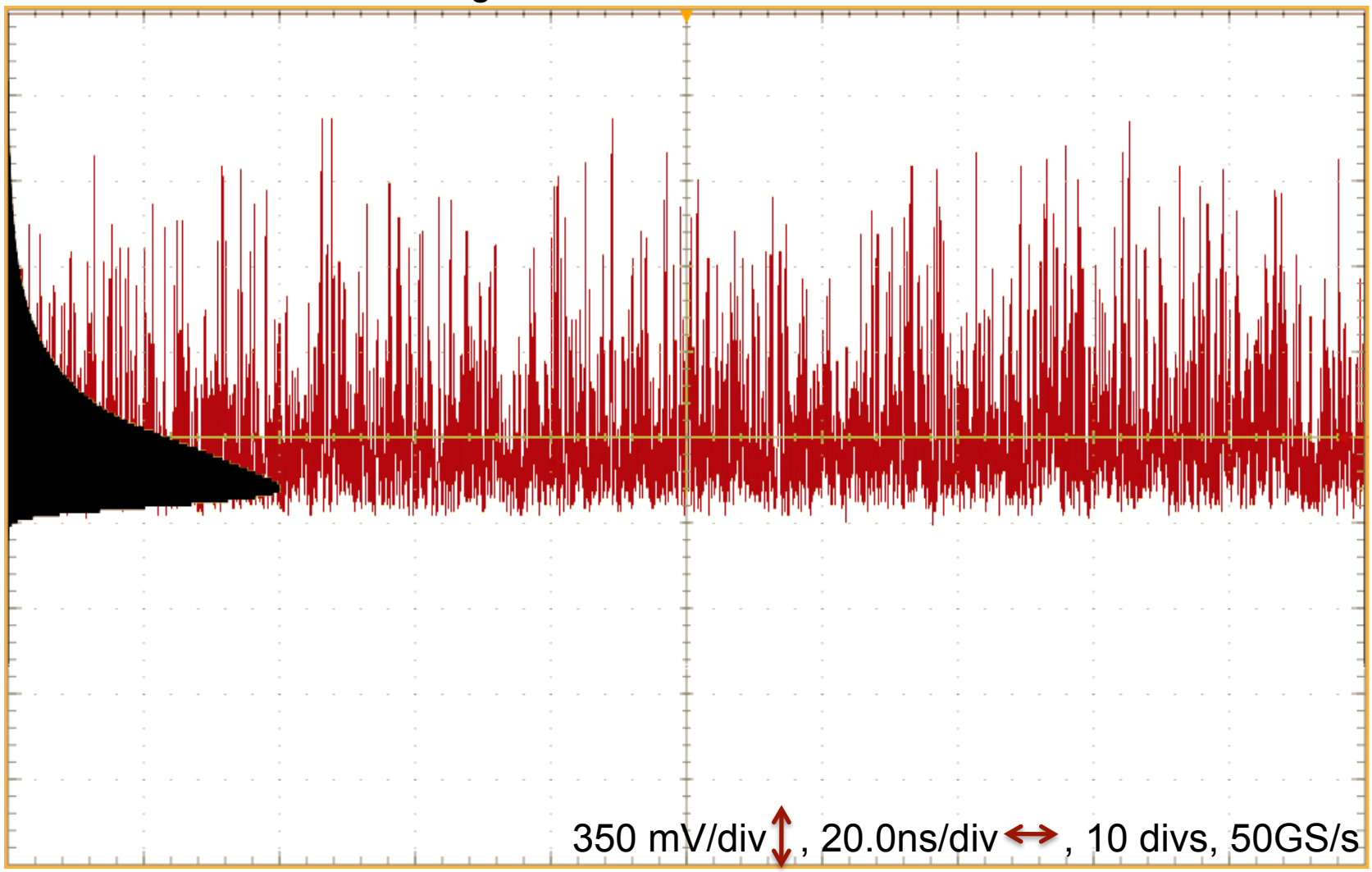
- Many applications require random numbers
  - Cryptography
  - Monte Carlo simulations
- Computer-based pseudo-random number generators – fast, but deterministic
- Hardware-based random number generators
  - Atmospheric noise
  - Photon counting
  - **Amplified spontaneous emission**

System


ASE Source
Preamplifier
Polarization Splitter
PD1
TIA1
BERT
Output
Er:Yb
EDFA
ATT1
TE
x
0 1 1 0 1 0
ATT2
TM
x̄
CLK
PD2
TIA2
Bandpass Filter (FBG)
(λ0 = 1552.5 nm, Δλ = 0.1 nm)
12.5 GHz

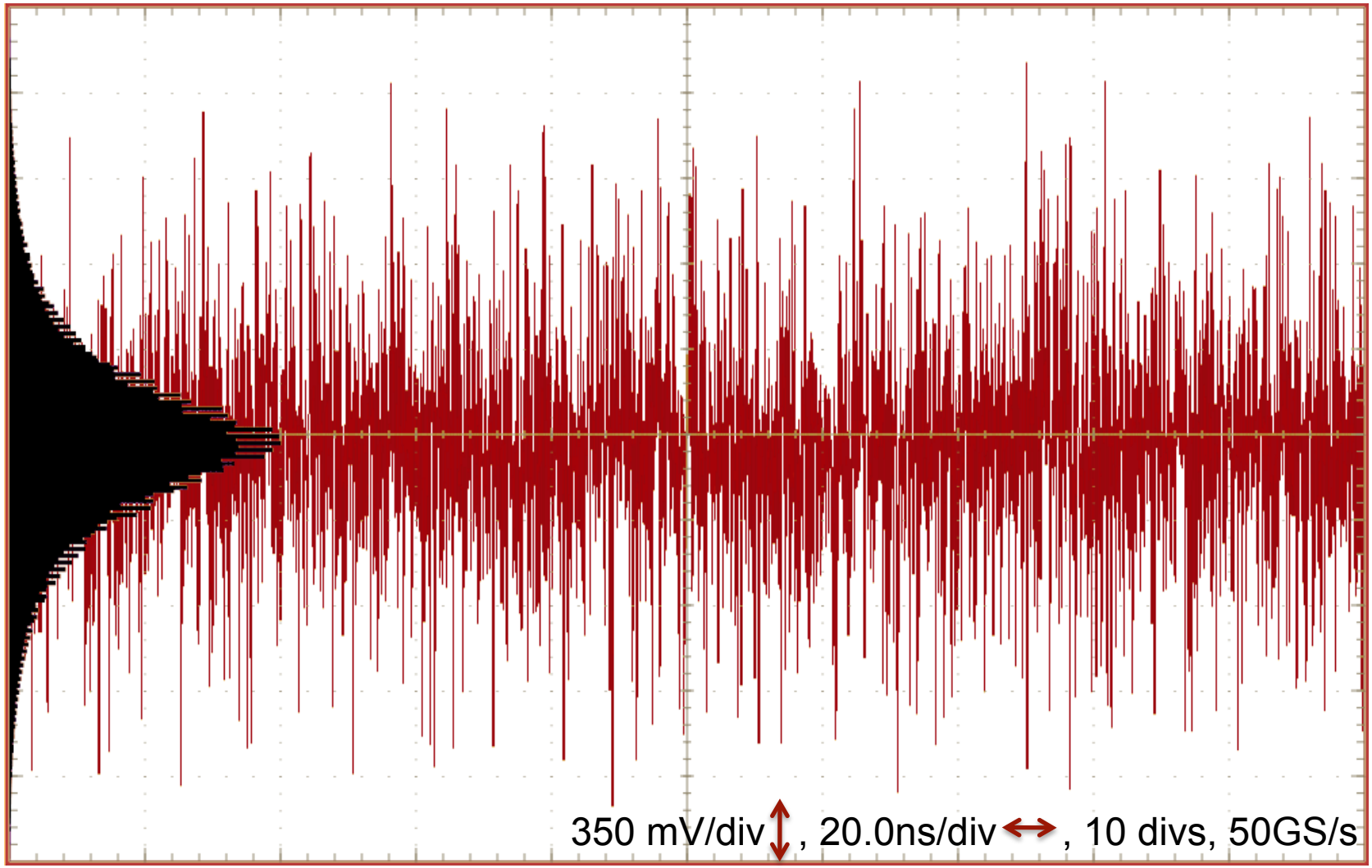
System

Single-sided Time Trace, 200ns



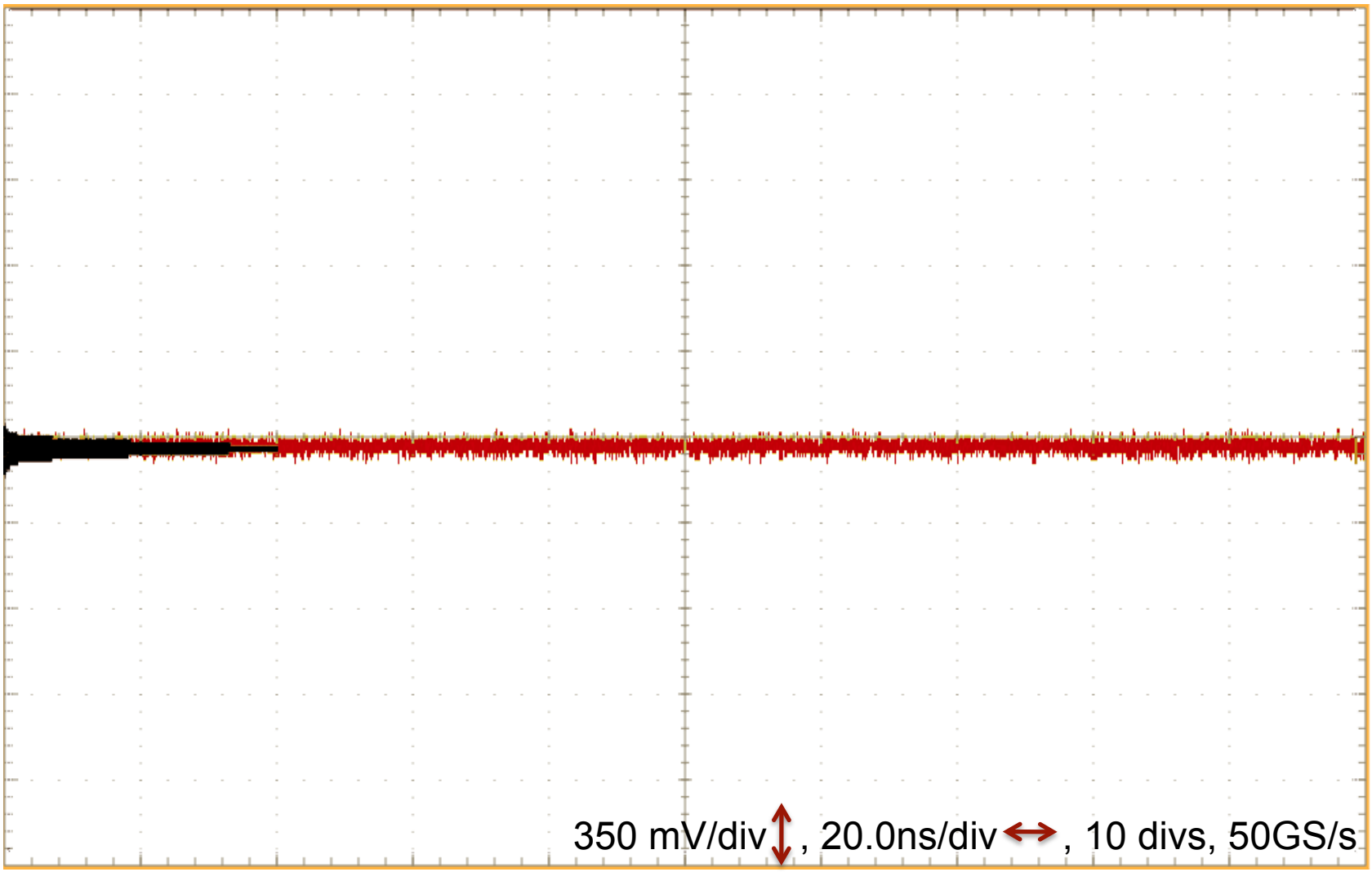
System

Differential Time Trace, 200ns

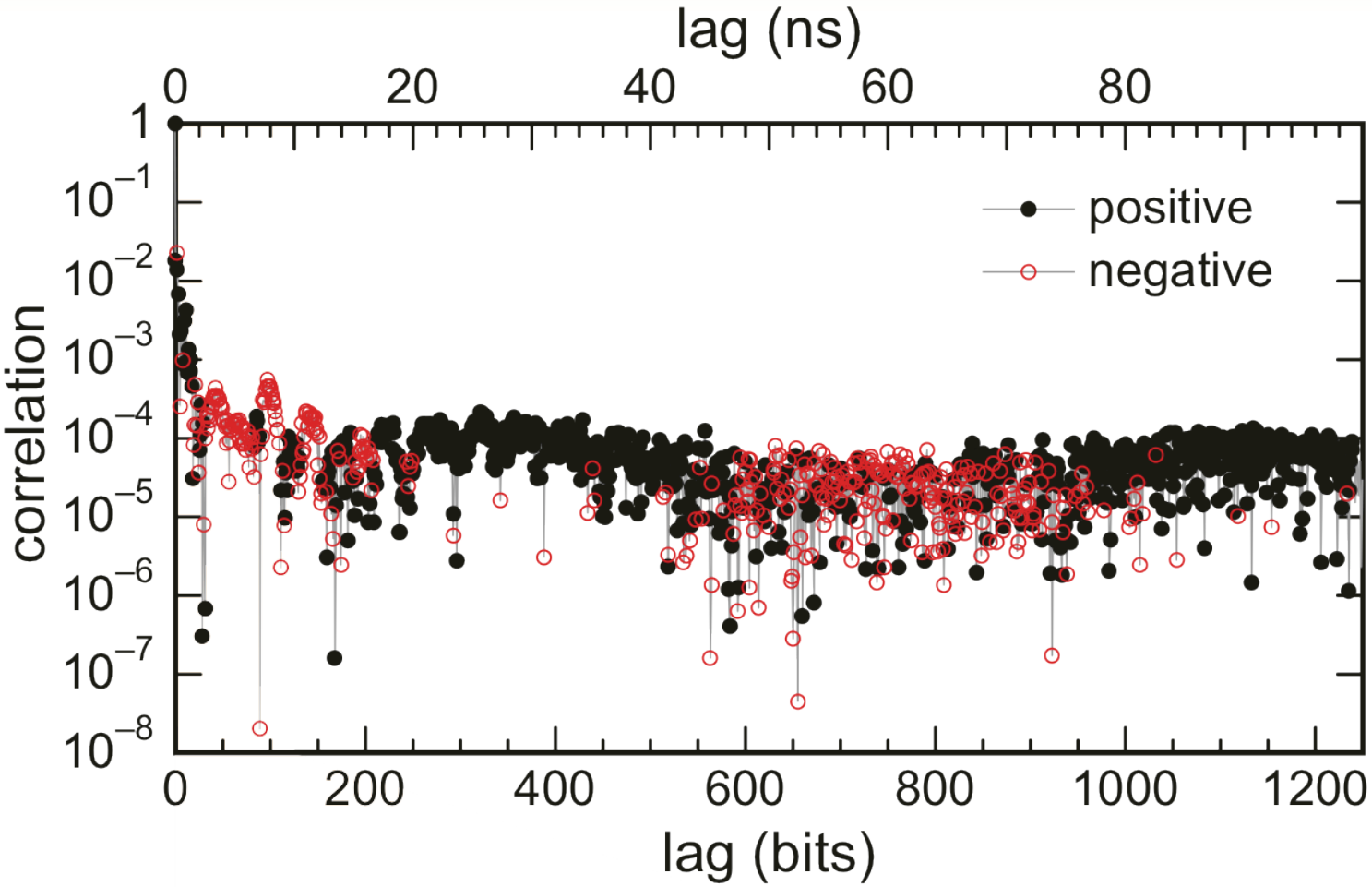


System

Electrical Noise Time Trace, 200ns



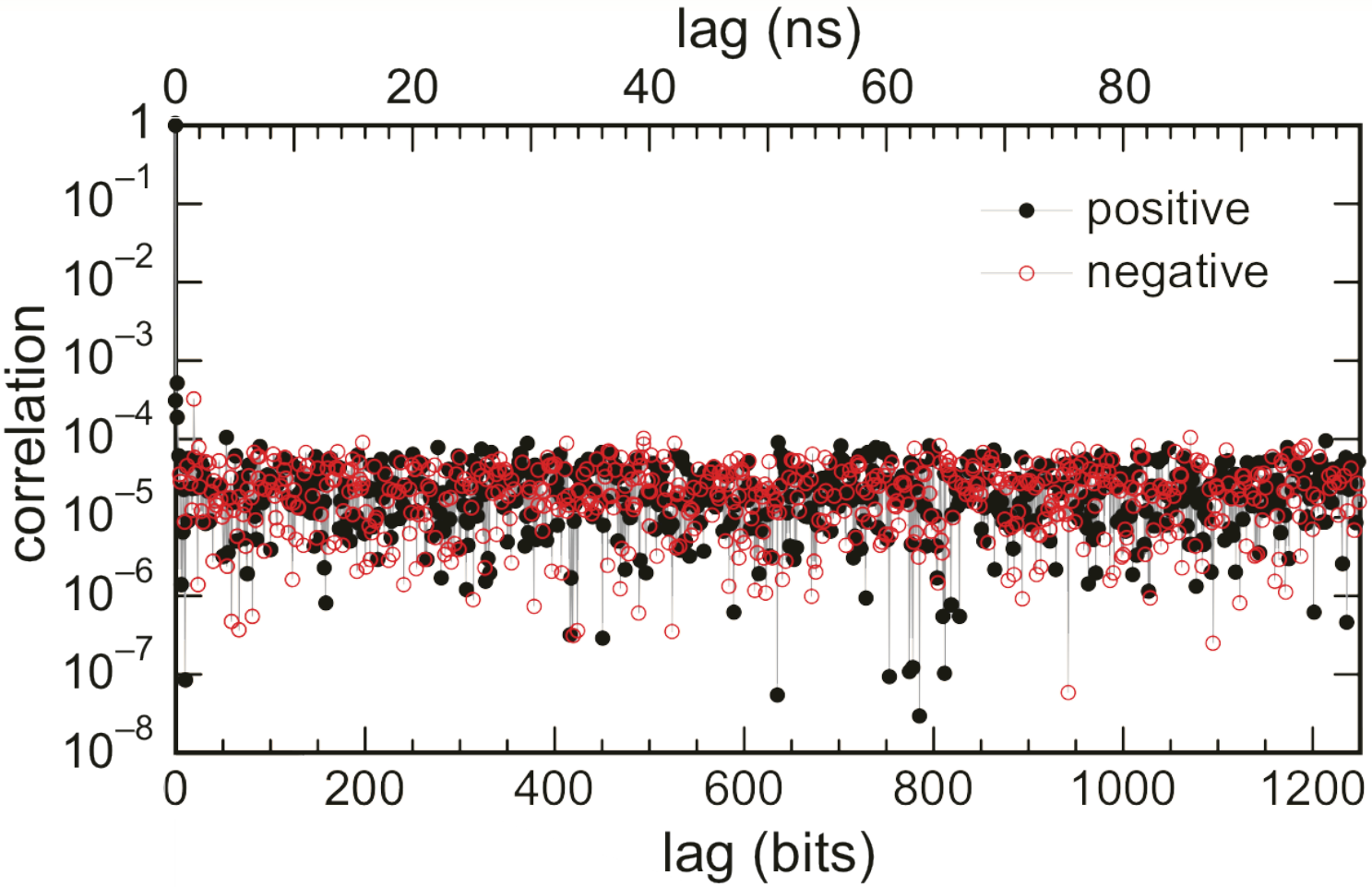
Results



Raw 12.5 Gbits/s data

- Large correlations at small lags
- Patterns across longer lags

Results

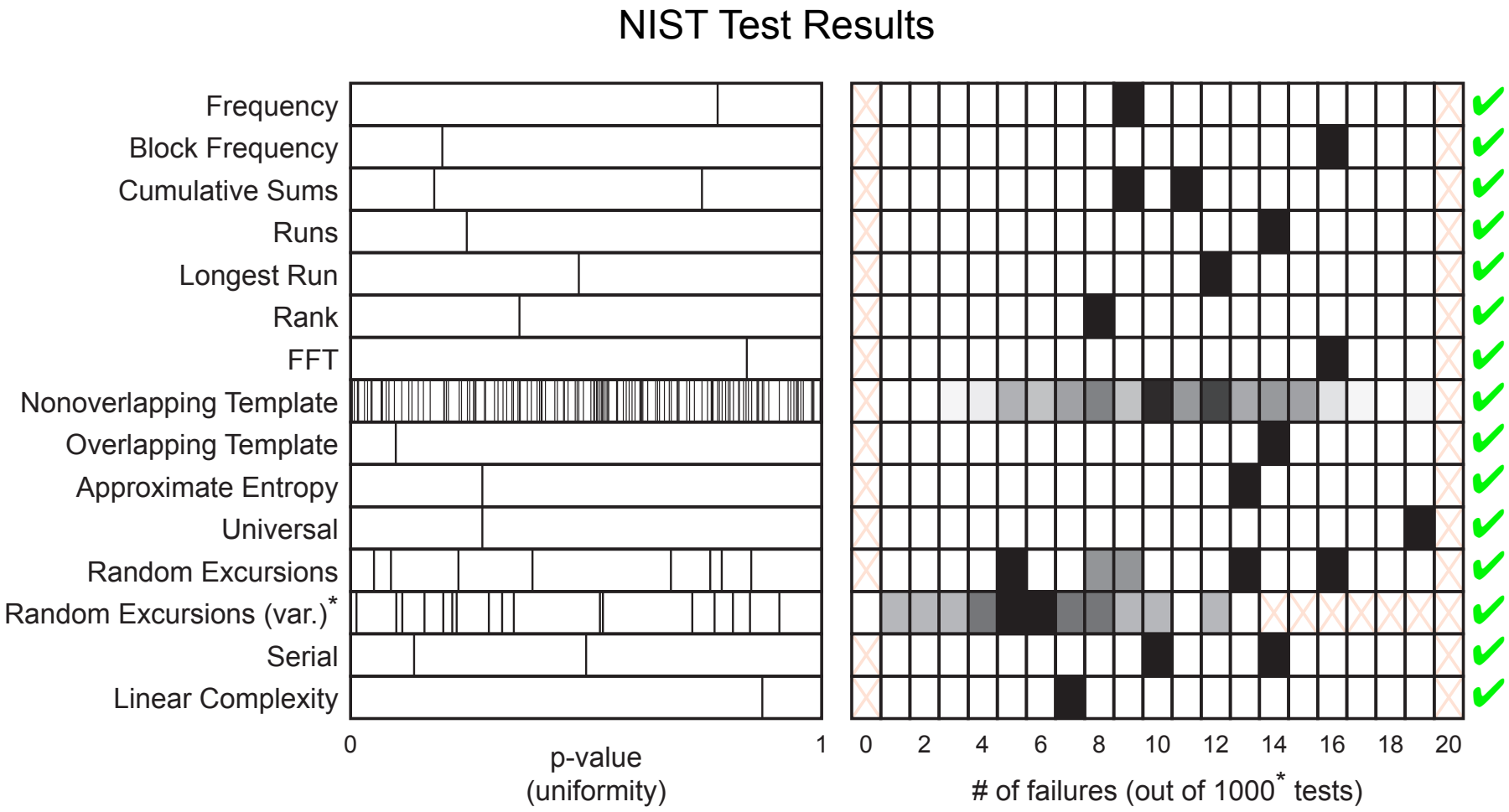


Raw 12.5 Gbits/s data
- Large correlations at small lags
- Patterns across longer lags

→

12.5 Gbits/s data, shifted with XOR
- Correlations reduced
- No obvious patterns

Statistical Testing



Conclusions

- High-speed (12.5 Gbits/s), physical random number generator
- Implementable entirely in hardware
- Passes stringent tests required for cryptographic security

Future Work

- Automate data acquisition
- Shielding from electromagnetic and other interference
- LED or other incoherent sources
- Scale system to multiple wavelengths