ABE-Style Threat Vectors Against Classical Computers & IoT

This whitepaper introduces how Aharonov–Bohm–style phase perturbations could be applied to classical computing systems. It examines attack vectors on PLLs, clocks, power delivery networks, wireless subsystems, crypto engines, and IoT sensors. It also describes mitigation strategies for system designers and CISOs.

Key Points:

- Vector potentials and low-level phase noise can introduce timing errors in CPUs and memory subsystems.
- Structured interference can disrupt wireless communications and force reconnects.
- Crypto engines may leak secrets under fault conditions induced by phase bias.
- IoT sensors may be spoofed to cause false triggers or disable safety features.

Mitigation Roadmap: Shielding, clock hardening, power monitoring, ECC protection, sensor fusion, and environmental monitoring.