Session 13 - Reliability of Systems and Devices - Focus Session: Reliability and Security in Circuits and Systems
Tuesday, December 10, 9:00 a.m.
Continental Ballroom 4
Co-Chairs: G. Konstadinidis, Google
G. Sethi, Amazon

9:05 AM **13.1** Challenges in Radio Frequency and Mixed-Signal Circuit Reliability (Invited)
Vijay Reddy, Samuel Martin, Kamel Benaissa, Cathy Chancellor, Karan Bhatia, Venkatesh Srinivasan, Vijay Rentala, Srikanth Krishnan, James Ondrusek, Texas Instruments

Reliability challenges encountered during the design of radio frequency (RF) and mixed-signal circuits are discussed. RF circuits can operate at voltages greater than twice the supply voltage and thus hot-carrier/off-state stress degradation are key considerations. Mixed-signal circuits also present a reliability challenge due to their stringent matching and offset requirements.

9:30 AM **13.2** Telemetry for System Reliability (Invited)
Robert Kwasnick, Hermann Gartler, Josh Boelter, John Holm, Sheela Surisetty, Chansik Im, Praveen Polasam, Oren Zonensain, Intel Corporation

Computer systems must be highly reliable for satisfactory user experience. Telemetry enables gathering actionable data from users. We review using field data to decide use conditions for IC reliability modeling and optimizations. Then we present concepts and results about telemetry for IC health monitoring, focusing on issue detection and support.

9:55 AM **13.3** Enabling Prognostics of Robust Design with Interpretable Machine Learning (Invited)
Jay Sarkar, Cory Peterson, Western Digital Corporation

Robust systems need to account for physics of operational stresses across the life cycle. This research demonstrates analysis of system-internal parametric data of Solid-State Storage Devices with interpretable Machine Learning (ML) - as effective and novel means of proactive prognostics - with significant possibilities across novel usage and application areas.

10:20 AM **13.4** Security and Reliability – Friend or Foe (Invited)
Ingrid Verbauwhede, Kai-Hsin Chuang, KU Leuven, imec

Security and reliability are more closely related than one might expect. This paper studies interesting research topics at the boundaries between the two domains. Reliability concerns can benefit security, e.g. to improve the performance of PUFs. Reliability issues can also trigger new security breaches, e.g. enabling Rowhammer attacks.

10:45 AM *COFFEE BREAK*

11:10 AM **13.5** Designing Secure Cryptographic Circuits (Invited)
Naofumi Homma, Tohoku University

Hardware security in mobile and embedded systems is drawing much attention in recent years. In particular, a variety of side-channel attacks on cryptographic circuits have been reported until now. This paper

introduces the design of cryptographic circuits resistant to side-channel attacks, including the-state-of-the-art side-channel attacks and circuit-level countermeasures.

11:35 AM **13.6** Leveraging Circuit Reliability Effects for Designing Robust and Secure Physical Unclonable Functions (Invited)
Chris Kim, Minsu Kim, Gyusung Park, Po-wei Chiu, University of Minnesota

Reliability mechanisms are undesirable from a product lifetime viewpoint, but their unique characteristics can enable novel applications. In this invited paper, we will discuss how reliability mechanisms can be leveraged for various circuit applications, and present a novel SRAM PUF where metal fuses are utilized for improved stability.

12:00 PM **13.7** Custom CMOS and Post-CMOS Crossbar Circuits for Resource-Constrained Hardware Security Primitives (Invited)
Kaiyuan Yang, Rice University

Securing ubiquitous resource-constrained systems in emerging applications faces severe hardware constraints on power and costs. In this paper, we present a suite of hardware security primitives, exploring crossbar circuits in CMOS and post-CMOS process, to lay a reliable and energy-efficient foundation for system security.