

The 6th IEEE Circuits and Systems Standard Activities Workshop



In conjunction with
The 33rd IEEE International Conference on Electronics, Circuits and Systems, 2026

Workshop title: TL-RNG 2026 – Trust Level Framework for TRNG & QRNG Systems: Toward the First IEEE Trust Certification Framework for Hardware Random Number Generators.

Venue: "SIROCCO" conference room, The MET Hotel, Thessaloniki, Greece.

Date and time: 8 November 2026.

Time: 13:30pm to 17:00pm (UTC+3).

Region: 08 (Africa, Europe, Middle East).

Time	Activity
13:30 – 13:40	Opening Ceremony
13:45 – 14:00	"From Randomness to Trust: Why We Need an IEEE Standard for TRNG and QRNG Systems" By: Dr. Hossam O. Ahmed, The American University of the Middle East, Kuwait.
14:00 – 14:30	"Trustworthy Randomness in AI-Driven Secure Systems: Threats, Requirements, and Architectures", Prof. Dr.-Ing. Elif Bilge Kavun, TU Dresden, Germany.
14:30 – 15:00	"SHU: Securing Hardware Unpredictability — From Entropy Evidence to Runtime Trust in Reconfigurable Systems", Prof. Mohamed El-Hadedy, California State Polytechnic University, Pomona, USA.
15:00-15:30	Coffee break
15:30-15:35	Pre-recorded invited presentation: "From Physical Labs to Digital Twins: Building Trustworthy Remote Engineering Environments", Prof. Rania Hussein, University of Washington, USA.
15:35-15:40	Pre-recorded invited presentation: "Evaluating TRNGs for Hardware Security: Entropy, Robustness, and Trust", Dr. Zain Ul Abideen, University of Idaho, USA.
15:40 – 16:00	"Beyond Noise: Bioelectronic Interfaces as Emerging Entropy Sources", Dr. Maryam Habibollahi, University College London, UK.
16:00 – 16:35	Panel Discussion on: Trust Level Framework for TRNG & QRNG Systems Dr. Yi (Estelle) Wang, AUMOVIO, Singapore (Panel moderator). - Prof. Dr.-Ing. Elif Bilge Kavun, TU Dresden, Germany. - Dr. Vasileios Tenentes, University of Ioannina, Greece. - Prof. Mohamed El-Hadedy, California State Polytechnic University, USA. - Dr. Ing. Nikolaos Athanasios Anagnostopoulos, University of Passau, Germany. - Dr. Hossam O. Ahmed, The American University of the Middle East, Kuwait.
16:35 – 16:45	IEEE Standard Activities Boon Chong Ang (Intel, Malaysia), IEEE CASS SASD, Chair.
16:45 - 17:00	Awards and Recognition Ceremony
20:00 – 22:00 PM	Workshop's Gala Dinner

***Note:** This table is subject to any modifications.

Links: <https://ieee-cas.org/society-involvement/overview/standards-activities>

Workshop General Chair:

- Boon Chong Ang, SASD Chair.
- Yi (Estelle) Wang, SASD Chair-Elect.
- Hossam O. Ahmed, SASD Voting Member.

Speakers, Panelists, and Program/ Technical Chairs



Name: Prof. Dr.-Ing. Elif Bilge Kavun

Affiliation: TU Dresden, Germany

Topic: Trustworthy Randomness in AI-Driven Secure Systems: Threats, Requirements, and Architectures

Abstract: Randomness forms the base of cryptographic security, privacy, and the reliable operation of many digital systems, yet its quality and trustworthiness are often difficult to assess once a hardware source is integrated into a product. In AI-driven secure systems, randomness serves different purposes, from model initialization and stochastic sampling to cryptographic key generation and privacy-preserving noise generation, each with different requirements. In this talk, we discuss the practical challenges of using Random Number Generators (RNGs), from physical entropy sources and changing operating conditions to health monitoring, conditioning, and software interfaces. Rather than treating statistical test results as the sole or main proof of security, we will also consider what evidence is needed to understand an RNG's assumptions, detect failures, and use its output safely. We will outline a set of practical trust requirements that apply to real deployments, including the integration of randomness into AI-driven secure systems, and conclude with a brief perspective on how evaluation practices could help guide future IEEE discussions.

Bio: Prof. Dr.-Ing. Elif Bilge Kavun is the leader of the Secure Digital Systems (SDS) research group at Barkhausen Institut and holds the Chair of Secure Digital Systems at the Faculty of Computer Science, TU Dresden, Germany. Previously, she held assistant professor positions at the University of Passau (DE) and The University of Sheffield (UK) and also worked as a Digital Design Engineer for Crypto Cores at Infineon (DE). She completed a PhD in Embedded Security in 2015 at the Faculty of Electrical Engineering and Information Technology, Ruhr University Bochum (DE). Her research focuses on the security of digital systems, particularly secure hardware, resource-efficient cryptographic primitives, fault-tolerant architectures, and the protection of AI-driven systems from both internal and external manipulation. She aims to develop robust, trustworthy technologies that maintain their integrity even under adversarial or mission-critical conditions.



Name: Prof. Mohamed El-Hadedy

Affiliation: California State Polytechnic University, Pomona, USA.

Topic: SHU: Securing Hardware Unpredictability — From Entropy Evidence to Runtime Trust in Reconfigurable Systems

Abstract: Hardware random number generators rely on characterized physical entropy sources whose behavior varies with operating conditions. Existing regimes—including NIST SP 800-90B/C and BSI AIS 20/31—recognize this dependence through characterization of permitted operating conditions and runtime health or online testing. This talk examines a complementary enforcement question: how can continued entitlement to an entropy claim be explicitly bound to demonstrated occupancy of the physical operating envelope under which its supporting evidence was established?

We investigate evidence-bound runtime trust on reconfigurable hardware, where placement, fabric activity, configuration, and environment can influence physical noise behavior, and where space and autonomous deployments may encounter conditions not represented during characterization. Source-level entropy measurements are associated with characterized operating regions; voltage, temperature, configuration, and fabric state serve as context and health evidence, never additional entropy. Output remains entitled only while the applicable evidence and freshness conditions hold; departure from the characterized envelope invokes fail-closed behavior rather than attempting to recover confidence through conditioning or output statistics.

Bio: Mohamed El-Hadedy is a Professor of Electrical and Computer Engineering at Cal Poly Pomona and Director of the Reconfigurable Space Computing Lab (RSCL). His research focuses on reconfigurable computing, cryptographic hardware, security and trust, dependable computing, and FPGA-based systems for autonomous and space applications. He holds a research appointment at the Coordinated Science Laboratory, University of Illinois Urbana-Champaign, and is a Senior Member of the IEEE/ACM.



Name: Dr. Maryam Habibollahi

Affiliation: University College London, U.K.

Topic: Beyond Noise: Bioelectronic Interfaces as Emerging Entropy Sources

Abstract: Hardware random number generators typically rely on electronic noise within a circuit for their unpredictability. This talk offers a different perspective, grounded in bioelectronic instrumentation. Physiological signals, picked up through electrodes and shaped by tissue-electrode interfaces and low-noise analog front ends, carry variability that originates in biology rather than in the electronics itself. A simple question follows: as this variability passes through the instrumentation chain, is it preserved, or filtered out along the way?

Drawing on recent examples of extracting randomness from physiological signals and from silicon-based alternatives, I examine this problem from the instrumentation side, looking at how electrode behavior, impedance, and front-end design shape what reaches the output, and where current evaluation methods may fall short of capturing what happens at that interface.

I close by turning the question around: rather than asking only how physiological signals might serve hardware security, I ask whether the degree of variability in such a signal itself could be informative, a possible marker of tissue condition or physiological state worth studying in its own right.

Bio: *Maryam Habibollahi (Member, IEEE) received the M.Eng. degree in electronic and electrical engineering in 2019 and the Ph.D. degree in 2024, both from University College London (UCL), London, U.K., where she was awarded an EPSRC Studentship to pursue her Ph.D. Since 2023, she has been a Research Fellow in Integrated Bioelectronics with the Bioelectronics Group, UCL. Her research interests include the design and development of active interface systems with integrated CMOS analog and mixed-signal circuits for biomedical applications.*



Name: Hossam O. Ahmed

Affiliation: American University of the Middle East (AUM), Kuwait.

Topic: From Randomness to Trust: Why We Need an IEEE Standard for TRNG and QRNG Systems

Abstract: Randomness is a fundamental building block of modern cryptographic and hardware security systems, supporting applications ranging from key generation and secure communications to trusted computing and emerging secure AI architectures. True Random Number Generators (TRNGs) derive entropy from physical nondeterministic phenomena, while Quantum Random Number Generators (QRNGs) exploit the intrinsic probabilistic nature of quantum measurements. Despite significant advances in both technologies, establishing the trustworthiness of an RNG remains a

challenging problem. Existing evaluation methodologies, including statistical randomness testing and entropy estimation, provide essential evidence about the quality of generated bitstreams, but passing statistical tests alone does not necessarily establish the security, robustness, or reliability of the complete RNG system. Factors such as entropy-source integrity, implementation architecture, conditioning, environmental variations, fault and attack resilience, health monitoring, restart behavior, and reproducibility must also be considered.

This introductory presentation discusses the fundamental principles of TRNGs and QRNGs and examines the gap between randomness validation and system-level trust. It motivates the need for a unified IEEE framework capable of defining common terminology, evaluation criteria, validation procedures, and trust levels for hardware random number generators. The presentation introduces the motivation and objectives of TL-RNG 2026, proposing a community-driven discussion toward an IEEE standard for the Trust Level Classification and Validation of Hardware Random Number Generators. The ultimate goal is to move from simple pass/fail statistical assessment toward a systematic, evidence-based approach for establishing and communicating the level of trust associated with TRNG and QRNG systems.

Bio: (M'14–SM'21) received the B.S. degree in communications and computer engineering from El-Shorouk Academy, Egypt, in 2007. He completed his M.Sc. and Ph.D. degrees in electronics and electrical communications engineering at Ain Shams University, Egypt, in 2015 and 2019, respectively. He is currently an Assistant Professor with the Department of Computer Engineering, American University of the Middle East (AUM), Kuwait. His research focuses on hardware security and emerging random number generation techniques, including True Random Number Generators (TRNGs) and Quantum Random Number Generators (QRNGs), as well as SPAD-based photon-timing systems and Time-to-Digital Converters (TDCs). His broader interests include FPGA/ASIC design, post-quantum cryptography, wireless sensor networks, AI hardware accelerators, intelligent control, and fuzzy systems. Dr. Ahmed is an active voting member of the Standards Activities Subdivision (SASD), IEEE Circuits and Systems Society, and contributes to the IEEE Standards Association (IEEE-SA) (2024–present).



Name: Vasileios Tenentes

Affiliation: University of Ioannina, Greece

Bio: Vasileios Tenentes (Member, IEEE) received the B.Sc. degree in computer science from the University of Piraeus, Piraeus, Greece, in 2003; and the M.Sc. and Ph.D. degrees in computer science and engineering from the University of Ioannina, Ioannina, Greece, in 2007 and 2013, respectively.

He is currently an Associate Professor in digital systems with the Department of Computer Science and Engineering at the University of Ioannina in Greece. In the past, he was a Research Engineer at Siemens (2007-2008), and at Helic, S.A. (2008-2009) in Athens (which was acquired by Ansys Inc., and then by Synopsys Inc.); a Research Fellow at the University of Southampton at the U.K. (2013-2017); and a

Research Engineer at Arm Ltd. in Cambridge, U.K. (2017-2018).

He has coauthored over 45 papers published in international journal and conference proceedings and holds 3 patents on hardware and systems security. His research interests include electronic design automation, hardware design for security, VLSI design and test, embedded systems and IoT, emerging VLSI technologies, and post-von Neumann computing architectures for emerging applications. His research has been nominated 3 times for best paper awards at IEEE conferences (ICECS'23, MOCAS'T'21, DFT'17) and has received a best paper award at ICECS'23. He has received funding by Arm Ltd., Bizzcom S.A., Census S.A., EPSRC, the EU (through Horizon and IPCEI) and Greek National resources. He has served at the technical program committee of many conferences (IEEE/ACM DATE, IEEE ICECS, IEEE MOCAS'T, IEEE ISCC and PACET) and is a member of IEEE (2007), TTTC of IEEE Computer Society (2007), CASS (2023) and HiPEAC (2023).



Name: Dr. Yi (Estelle) Wang

Affiliation: AUMOVIO, Singapore.

Bio: Dr. Yi (Estelle) Wang received the B.S. and M.S. degree from Northwestern Polytechnical University, Xi'an China in 2000 and 2003, and the Ph.D. degree from Nanyang Technological University, Singapore 2008. From August 2025, she worked as Global Head of Consulting and Engineering and Head of Product Cybersecurity & Privacy Office (PCSO) Singapore, at AUMOVIO Automotive (Note: previously known as "Continental Automotive Singapore", Joined Continental from 2016). Dr. Wang is in charge of six locations around the world focusing on product consulting and engineering and leading four teams at Singapore: the advanced research in security and privacy team, product governance team, consulting and engineering team, and the product

operations team. In addition, she is with deep knowledge of ISO/SAE 21434 and UNECE R155/R156 based on physically participating in working group meetings. She is an expert with cybersecurity industrial standards, e.g., ISO 2700x and ISO 26262. She is familiar with data protection and privacy regulations: GDPR and Asia regional regulations (Singapore PDPA and Chinese PIPL). Advanced leading research topics are including but not limited to quantum-safe applications, applied lightweight cryptography, embedded security for IoTs, cybersecurity for artificial intelligence (adversarial model), privacy enhancing technology (data anonymous, federated learning) for automotive.



Name: Boon Chong Ang

Affiliation: INTEL, Malaysia.

Bio: Ang Boon Chong was born in Penang, Malaysia, in 1978. He received the B.E. degree in microelectronic engineering from the University Putra Malaysia, Malaysia, in 2002, and MBA from Open University Malaysia, Malaysia in 2014. He is currently affiliated with Intel Malaysia, been engaged in a wide variety of advanced nodes and methodology evaluation. He has published over 40 papers as well as delivered 2 invited talks in 2 countries. He is currently a tech lead within the organization as well as IEEE senior member. He is a Senior Member of the IEEE and currently serves as Chair (2026–present) of the IEEE Circuits and Systems Society, Standards Activities Subdivision (SASD).



Name: Nikolaos Athanasios Anagnostopoulos

Affiliation: University of Passau, Germany

Bio: Nikolaos Athanasios Anagnostopoulos (Senior Member, IEEE) received the B.Sc. degree in computer science from Aristotle University of Thessaloniki, Greece, in 2012, the M.Sc. degree in computer science from the University of Twente, The Netherlands, in 2014, the M.Sc. degree in innovation in information and communication technology from the Technical University of Berlin, Germany, in 2014, and the Dr.-Ing. degree in computer science from the Technical University of Darmstadt, Germany, in 2022. He is currently a post-doctoral researcher with the Chair of Computer Engineering, University of Passau. His research interests include physical and hardware security, with a focus on commercial electronics, Physical

Unclonable Functions (PUFs), True Random-Number Generators (TRNGs), the Internet of Things (IoT), and chaos-based cryptography. He is the Chair of the German Chapter of the IEEE Consumer Technology Society; the Vice Chair of the German Chapter of the IEEE Circuits and Systems Society, the German Chapter of the IEEE Solid-State Circuits Society, the German Chapter of the IEEE Vehicular Technology Society, and the German Chapter of the IEEE Computational Intelligence Society; as well as the Secretary of the German Chapter of the IEEE Computer Society. Additionally, he is also a member of ACM, IACR, GI, KIVI, VDE, VDI, and AMS. For more information, see <https://www.anagnostopoulos.academy/>.



Name: Prof. Rania Hussein

Affiliation: University of Washington, USA.

Bio: Rania Hussein is a Teaching Professor, the Founder and Director of the Remote Hub Lab (RHLab), and an Associate Director of the UW Industrial Assessment Center (IAC). Her research focuses on embedded systems, digital twinning, remote engineering, medical image analysis, and engineering education. She currently serves as the chair of the UW Faculty Senate for the year 2026-2027.

She has over 15 years work experience in higher education as an educator and mentor to hundreds of students and alumni of electrical and computer engineering and computer science. Before joining UW, she was a research engineer at the Walt Disney Company where she worked on software development and the evaluation of

disruptive and cutting edge technologies. In addition to her technical expertise, Dr. Hussein has extensive experience in project management and community leadership. She has served as a founder, board member or executive director for non-profits to promote diversity, equity, and inclusion. She contributed to the building and passing of SB-5166 Bill into WA State law in 2019. This law requires post-secondary institutions to provide alternate exam accommodation for students due to religious observance. This accommodation became part of the syllabi of higher educational institutions in the State of WA. Dr. Hussein is an award-winning educator who has been nationally recognized for her contribution to mentorship and research in engineering education. She is the recipient of the Innovative Program Award from the Electrical and Computer Engineering Department Heads Association (ECEDHA) of 2021. She is also the recipient of IEEE region 6 outstanding engineering educator, mentor, and facilitator in the area of STEM award for the year 2022.



Name: Dr. Zain Ul Abideen

Affiliation: University of Idaho, USA.

Title: Evaluating TRNGs for Hardware Security: Entropy, Robustness, and Trust

Abstract:

Trust in a hardware random number generator depends on its physical source, evaluation assumptions, and the implementation that delivers its output. This talk introduces oscillator jitter, metastability, electronic noise, and quantum measurement approaches, then relates their evaluation to the NIST SP 800-90 series and current BSI AIS 20/31 criteria, including PTG.2 and PTG.3. Published studies illustrate how stochastic model assumptions, correlations, adversarial observations, and injected disturbances affect entropy claims and design decisions. The discussion links failure

detection and output release to a conditional min-entropy budget and the assumptions required for randomness extraction. A homodyne quantum random number generator provides a final example, showing how measurement electronics, ADC characterization, and seed quality enter the security assessment. Overall, the talk proposes evaluating trust through explicit source assumptions, verified implementation behavior, and design vs. security overheads.

Bio: Dr. Zain Ul Abideen's research focuses on hardware security while ensuring the trust and security of integrated circuits (ICs), addressing challenges in secure chip design, system integrity, and privacy. His research interests span security-aware electronic design automation (EDA) protection against reverse engineering, circuit obfuscation,

and post-quantum cryptographic accelerators. He also develops hardware security primitives such as physical unclonable functions (PUFs) and true random number generators (TRNGs), alongside fault-tolerant digital systems and machine learning/AI-assisted chip design. Prior to joining the University of Idaho, Dr. Abideen was a researcher in the Department of Electrical and Computer Engineering at Carnegie Mellon University (CMU). He holds a Ph.D. in Information and Communication Technology from Tallinn University of Technology, Estonia.