Title: Unlocking the future: Intel HERACLES and The Dawn of Encrypted Computing

Speaker: Ro Cammarota (Intel Labs)

Abstract: In our data-driven world, where information is both vast and invaluable, the need for innovative protection methods has never been greater. Enter encrypted computing—an extraordinary frontier of encryption techniques and cutting-edge hardware and software. It offers the remarkable ability to perform direct operations on encrypted data without the need for decryption, revolutionizing data security as we know it.

Imagine a world where your data remains truly confidential, shielded from prying eyes and the ever-present threat of data breaches. Encrypted computing holds this potential. It not only safeguards the privacy of data owners but also dramatically reduces the risk of data exposure.

Intel HERACLES emerges as a game-changing encrypted computing platform, setting the stage for a new era in data security. It accelerates fully homomorphic encryption, enabling native execution of ring polynomial arithmetic across the entire computing stack. In the realm of hardware, HERACLES boasts features like on-die twiddle factors and key-switch expansion, effectively minimizing metadata movement overhead for critical operations. On the software front, HERACLES seamlessly integrates state-of-the-art fully homomorphic encryption algorithms from renowned open-source libraries such as MSFT SEAL, OpenFHE, and LattiGo. Additionally, it introduces a domain-specific language, empowering fine-grained programming of the platform. Both the hardware and software components of HERACLES undergo rigorous formal verification, ensuring end-to-end correctness.

HERACLES doesn't just stop at innovation—it delivers unparalleled speed and efficiency, outperforming even the most advanced data center platforms. By reducing encrypted data processing overhead to within 10x of clear-text computation, HERACLES makes deploying fully homomorphic encryption solutions not just feasible but practical. It bridges the gap between aspiration and reality in encrypted data processing, setting new standards for data security.

Bio: Ro is a principal engineer and Chief Scientist of Privacy-Enhanced Computing Research in the Emerging Security Lab at Intel Labs. He leads the Encrypted Computing program at Intel. His work includes advancing theory, applications, and standardization of technologies for processing encrypted data. He is the principal investigator for the DARPA DPRIVE program and Intel academic centers focusing on privacy, cryptography, and security mechanisms. Ro is a prolific author and inventor, publishing over 65 peer-reviewed articles and opening more than 60 US patents. Ro Cammarota is a Senior Member of IEEE and recipient of the SRC “Mahboob Khan” Outstanding Industry Liaison Awards in 2017, 2018, and 2019. He received his Ph.D. in Computer Science from the University of California Irvine in 2013.