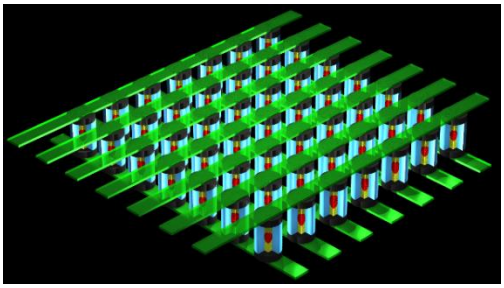
IBM Research –Zurich

Crytography meets in-memory computing



+

For decades, conventional computers based on the von Neumann architecture have performed computation by repeatedly transferring data between their processing and their memory units, which are physically separated. As computation becomes increasingly data-centric and as the scalability limits in terms of performance and power are being reached, alternative computing paradigms are searched for in which computation and storage are collocated. A fascinating new approach is that of computational memory where the physics of nanoscale memory devices are used to perform certain computational tasks within the memory unit in a non-von Neumann manner.

A fascinating new application for in-memory computing is in the domain of cryptography. Today, cryptography has become ubiquitous in modern computing systems. Cryptography helps provide confidentiality, authentication and integrity, among other properties for securing data at rest, in transit and in use. With ever growing amounts of data and reliance on computing systems for storing, communicating and using the data, protecting the data at scale with low latency and low energy consumption is challenging. In-memory computation opens up avenues to explore the possibility of performing low latency cryptography to meet the demanding needs of security at scale.

We are inviting applications from students to conduct their Master thesis work or an internship project at IBM Research – Zurich on this exciting new topic. The work performed could span low-level hardware experiments on world's first computational memory chips based on phase-change memory devices to high-level algorithmic development in the domain of cryptography. It also involves interactions with several researchers across IBM research focusing on various aspects of the project. The ideal candidate should have a multi-disciplinary background, strong mathematical aptitude and programming skills. Prior knowledge on emerging memory technologies such as phase-change memory is a bonus but not necessary.

If you are interested in this challenging position on an exciting new topic, please send your most recent curriculum vitae including a transcript of grades by email to:

Dr. Navaneeth Rameshan (vme@zurich.ibm.com) and Dr. Abu Sebastian (ase@zurich.ibm.com)

[1] A. Sebastian, M. Le Gallo, R. Khaddam-Aljameh *et al*. Memory devices and applications for in-memory computing. *Nature Nanotechnology* (2020). https://doi.org/10.1038/s41565-020-0655-z