

---

## SECURING DATA IN THE QUANTUM ERA

Rainer Steinwandt (Florida Atlantic University, [rsteinwa@fau.edu](mailto:rsteinwa@fau.edu))

At this point, large-scale quantum computers are not available yet, but several major commercial players, including Google, IBM, and Microsoft, are actively working towards harnessing the potential of this technology. On the side of data security, the availability of large-scale quantum computing means that several of today's solutions for ensuring integrity, confidentiality, and authenticity of data are no longer adequate. Consequently, the National Institute of Standards and Technology (NIST) initiated a standardization effort to develop *post-quantum* cryptographic solutions for some fundamental cryptographic tasks.

This talk will try to give a realistic (non-technical) view on the impact of quantum technology on data security and highlight some of FAU's work in this area.