



**Wednesday, October 6, 2021**

**Under the Hood of the Quantum Computer (1:00 - 1:50 pm EST)**

**SARR: A Cybersecurity Metrics and Quantification Framework (2:00 – 2:50 pm EST)**

Mark your calendar and come join us for CAE Forum! CAE Forum is a live, real-time, online, academic forum where members of the CAE community give non-technical presentations on topics of value to the CAE community. CAE Forum is about sharing your ideas, knowledge, and expertise to empower and strengthen our community. It's that simple. CAE Forum presentations are normally held on the third Wednesday of each month during the Fall and Spring semesters.

### **PRESENTATION #1**

**Title/Topic:** Under the Hood of the Quantum Computer

**Time:** 1:00 - 1:50 pm EST

**Location:** <https://caecommunity.zoom.us/my/caeforum>

*Just log in as "Guest" and enter your name. No password required.*

**Audience:** Students, Professors, Govt.

**Presenter(s):** Bruce Harmon, PhD, Professor, Computer Science, University of Denver

**Description:** Activity and research in quantum computing have been accelerating since breakthroughs a decade ago. The idea dates back to the 1980s when Richard Feynman and others proposed that the only way to simulate the reality of the quantum world would be with a quantum computer. That led to some fundamental research into what such a computer would be and what kinds of problems it would excel at. Among that list of problems is the factoring of public keys to extract the private keys for decryption. Such a capability could make useless the RSA algorithm currently widely used in encryption and decryption of data. In this talk, we go under the hood to see what a quantum computer, if it existed fully and at scale, would involve; how the RSA would be vulnerable to it; and some thoughts on mitigation.

### **PRESENTATION #2**

**Title/Topic:** SARR: A Cybersecurity Metrics and Quantification Framework

**Time:** 2:00 - 2:50 pm EST

**Location:** <https://caecommunity.zoom.us/my/caeforum>

*Just log in as "Guest" and enter your name. No password required.*

**Audience:** Students, Professors, Govt.

**Presenter(s):** Shouhuai Xu, University of Colorado, Colorado Springs

**Description:** Cybersecurity Metrics and Quantification is a fundamental but notoriously hard problem. It is no doubt one of the pillars underlying the emerging Science of Cybersecurity. In this talk, the presenter will describe a Cybersecurity Metrics and Quantification framework, dubbed SARR for Security, Agility, Resilience and Risk. The presenter will discuss a range of open problems for future research.

A recording of the live presentation will be available within 48 hours of the presentation at:

<https://www.caecommunity.org/content/cae-forum-resources>

**Contact us at:** [caeforum@caecommunity.org](mailto:caeforum@caecommunity.org)