## Department newsroom

### IEEE International Symposium on Information Theory conference

Dr. Malluhi and his collaborators were able to break a cryptographic algorithm that was proposed as a candidate to become a NIST Post Quantum Cryptographic standard. It is known that many of the cryptographic algorithms that are widely used today in our day-to-day online interactions will no longer be secure as quantum computers are moving closer and closer to becoming a reality. This is creating a big concern in the community as it implies that most of online services that we heavily rely on today would collapse. Therefore, the National Institute of Standards and Technology (NIST), a major standards organization, has recently initiated a process to establish a post-quantum resistant standard for public-key cryptography. After process round 1, a cryptographic algorithm called HK17 was one of the standard candidates. Dr. Malluhi and his collaborators were able to identify weaknesses in this standard candidate and showed a method for breaking it. This significant result has been presented in France in the renowned 2019 IEEE International Symposium on Information Theory (ISIT 2019), which is the top international conference in the area information theory.


## Visit to Oman

Prof. Malluhi also participated in the Workshop on the Future of Computing Programs at Sultan Qaboos University (SQU), Oman. The workshop was held on Oct 1, 2019. Dr. Malluhi was invited by SQU to this event in order to offer expert opinion and recommendations regarding possible future directions for structuring the different computing programs at SQU. Dr. Malluhi has delivered an invited talk and participated in round-table and panel discussions regarding recent trends in computing education and the future of computing programs.