Title: Achieving Private Information Retrieval Capacity in Distributed Storage Using an Arbitrary Linear Code

Speaker: Dr. Hsuan-Yin Lin, Simula@UiB, Bergen, Norway

Time and location: Friday, March 23, 2:30pm

Abstract:
In this talk, we will present a private information retrieval (PIR) protocol for distributed storage systems (DSSs) with noncolluding nodes where data is stored using an arbitrary linear code. An expression for the PIR rate, i.e., the ratio of the amount of retrieved stored data per unit of downloaded data, is derived, and a necessary and a sufficient condition for codes to achieve the PIR capacity are given. The necessary condition is based on the generalized Hamming weights of the storage code, while the sufficient condition is based on code automorphisms. We show that cyclic codes and Reed-Muller codes satisfy the sufficient condition and are thus PIR capacity-achieving.

Bio:
Hsuan-Yin Lin received his B.S. major degree in electrical engineering and minor degree in mathematics from National Tsing-Hua University (NTHU), Taiwan, in 2007, and his M.S. degree and Ph.D. degree in electrical and computer engineering from National Chiao Tung University (NCTU), Taiwan, in 2008 and 2013, respectively. From late 2014 to 2016, Dr. Lin was a visiting scholar at CYSEC, TU Darmstadt, Germany. Currently, he is a postdoctoral research fellow at Simula@UiB, Bergen, Norway.
In 2014, Dr. Hsuan-Yin Lin was awarded the Honor Membership of the Phi Tau Phi Scholastic Honor Society of the Republic of China (Taiwan). His research interests include coding in distributed storage systems, finite blocklength information theory, inference security and target localization in wireless sensor networks, and quantum error correcting codes.