MMC Reflection Report

19.09.2017

Bo Sun
University of Bergen

Overview

On 4-8 Sep this year, the workshop of Mathematical Methods for Cryptography (MMC) is organised by Selmer Center, Department of Informatics of University of Bergen at Svolvær of Lofoten in Norway. This workshop is also dedicated to celebrate professor Tor Helleseth's 70th birthday. Professor Helleseth is one of the most prestigious professors in cryptography world widely and I am lucky to work in the same group with him. Joining the conference this time is great honor to learn new knowledge and meet people at different cutting edge of cryptography, at meanwhile, as the witness of Tor's 70 years old birthday and his 100st paper published on IEEE. MMC this year was an international, high-level summit. 17 invited speakers from different fields of information security field and there were totally 60 participaters. Speakers include Kaisa nyberg, who introduced the theory of perfect nonlinear S-boxes, KN-Cipher and the cryptanalysis of the stream ciphers E0 and SNOW, Claude Carlet, famous cryptographer also and world leading expert in bent boolean field and Joan Daemen, one creator of AES and ect.

"Recent Advances in Doppler Resilient Sequence Design and Applications" by Professor Fan

➢ Presentation Content

Sequences with good correlation properties play vital role in wireless communications, radar sensing, and cryptography. To predict the range of the target from a radar based on the delay in the radar return. Furthermore, advances in circuit tech reinforced by new signal processing algorithms, machine learning, artificial intelligence and computervision tech have made self-driving cars a reality. Furthermore, advances in circuit tech reinforced by new signal processing algorithms, machine learning, artificial intelligence and computer vision tech have made self-driving cars a reality. Professor Fan introduced existing and new mechanisms to construct Doppler resilient sequences based Golay and Z-complementary sequences and radar radio used in mobility industry.

➢ Reflection to my research

Before this talk, I never knew radar is related to sequence and there are many criteria for choosing the right sequence for application. This presentation extended my vision of applicable cryptography.

“Characterizations of Differentially Uniform Functions by the Walsh Transform and Related cyclic difference set-like Combinatorial Structures” by Professor Carlet

➢ Presentation Content

Professor Carlet proved that quadratic and Kasami APN functions are componentwise Walsh uniform. The term Componentwise APN-ness (CAPNess) is introduced by professor Carlet, which is a stronger version of APN-ness related to the characterization by the fourth moment. Furthermore, inverse of one of the Gold functions, and deduce a new property of Kasami functions related to the difference set property proved by Dillon and Dobbertin in 2004.

➢ Reflection to my research

APN functions is a main research direction of my research, however, I never learned the Componentwise APN-ness before. Since I am writing my thesis, this term and result will be included in my thesis.

As I mentioned, there are 17 invited talks from different cutting edge in this workshop, due to the limit space here, I can’t mention every talk. Since this is an universal workshop for cryptography, many talks I can’t really understand, however, I believed attending and participating are always beneficial. Talking with many successful people, discussing and consulting promised future in this field with them, getting to know their time management and etc will have potential great benefits for us. These things seem trivial, however, these may change our future direction and personal life. For example, professor Fan jogged every morning for years. It says, “A fine example has boundless power”. I have started to jog every morning after coming back from Lofoten for developing my intellectual perseverance and body building. I never expect I will be as great as them, but I can try to be better myself by learning from them.