BFA Reflection Report

07.08.2017

—

Bo Sun
University of Bergen

Overview

On 3-8 July this year, the Boolean Functions and their Applications (BFA) is organised by Selmer Center of university of Bergen in Os in Norway. This workshop invited many most respected and people are in decisive position in this Boolean and bent function fields. For example, 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. I will two interesting talks and reflect how they facilitate my research.

"On APN Permutations" by Marco Calderini

➢ Presentation Content

Marco Calderini gave a talk named "On APN Permutations". He pointed out that APN permutations are completely characterized by the derivatives of their components. He and his colleagues proved that when n is even and characteristic is 2, APN permutation has no partially-bent (quadratic) component. However, an APN permutation in even dimension can have plateaued components. He reviewed the history people tried to find APN permutation in even dimension. In 2006, Hou conjectured that there is no APN permutation in even dimension, until 2009, Dillon presented an APN permutation in dimension 6. That APN permutation is equivalent to "Kim" function, which is useful tools for APN permutation research since in 2009, Browning, Dillon, McQuistan and Wolfe proved that "kim" function are CCZ-equivalent with APN permutation. He also introduced the facts between APN functions, APN permutations and codes, recent result which to construct APN permutation. In the end, he talked about open problems in this field.

➢ Reflection to my research

One part of my research is APN permutation, so this topic is quite in interesting to me. He concisely introduced the background and trend in this field, let me understand the knowledge systematically and know better between each founded results until now.

“On S-box Reverse-Engineering: from Cryptanalysis to the Big APN Problem” by Leo Perrin

➢ Presentation Content

Leo’s presentation is from different angle than directly use mathematics to check the big APN problem: except the only APN permutation case on GF(2^6), are there other APN permutations on GF(2^n) when n is even? Furthermore, their group can determine many structures of S-boxes and use their way to generalize the only APN permutation found by Dillon, however, these generalize functions(except the known cases) are not APN. They from the application of S-box to find new patterns of design of S-boxes.

➢ Reflection to my research

Although the results are never be APN functions, this method is very creative and imply that it is possible to search APN in other ways.