Crooked functions

Russell East, School of Mathematical and Geospatial Sciences,
RMIT University

Today in the world of cryptosystem design, it is generally required that any round function designed for a cipher, be resilient to both linear and differential cryptanalysis. Functions which present optimal resistance to differential cryptanalysis are referred to as being Perfect Nonlinear and in the case of binary cryptosystems are called Almost Perfect Nonlinear. A small class of these Almost Perfect Nonlinear functions are Crooked and these functions can also be resistant to linear cryptanalysis. As part of my vacation scholarship, I went about researching Crooked functions under the supervision of Professor Kathy Horadam at RMIT in Melbourne.

Crooked functions have been mainly studied due to their applications in the construction of resistant round functions in ciphers. Despite this application, I found after examining the available literature on Crooked functions, that they are still a relatively new, unexplored area of research and a common definition for them is absent. There are in fact a number of definitions for Crooked functions and in order to continue research on them, it would be reasonable to require that we know whether each of the definitions are conflicting or equivalent to one another.

This scholarship has been a great experience for many reasons. It has enabled me to get a taste of research before starting honours, it has given me an opportunity to practice my presentation skills, and it has allowed me to socialise with other like minded people from around the country at CSIRO's Big Day In this year.

As a result of this scholarship, I plan to continue with the same topic of research as my honours thesis. The research conducted during the scholarship period will form part of the literature review and for this headstart, I'm very grateful to both AMSI and MASCOS for having provided this opportunity.

Russell was an AMSI/MASCOS Vacation Scholar for 2007-8.