# Correlation Immune and Resilient Generalized Boolean Functions

*Thor Martinsen, PhD*
*Commander, United States Navy*
*Assistant Professor of Applied Mathematics & Cyber Security*
*Naval Postgraduate School, Monterey, California, USA*
*thor@nps.edu*

*7-22 June, 2018*

In this talk we extend the concept of correlation immunity and resiliency from the clasical Boolean functions case to the generalized Boolean function setting. In particular, we discuss a construction method capable of creating a large class of order 1 correlation immune or 1-resilient generalized Boolean functions. Subsequently we demonstrate how orthogonal arrays and linear codes can be employed to create higher order correlation immune and resilient generalized Boolean functions. Using these techniques we further discuss creating correlation immune Rotation Symmetric (RotS) generalized Boolean functions. We establish an upper bound on the number of possible correlation immune RotS functions, and demonstrate that no RotS generalized Boolean functions in $p$ variables with outputs in $\mathbb{Z}_q$ for odd prime $p$ and $q > 2$ can be constructed using our technique. Additionally, we extend the Siegenthaler correlation immunity construction technique so that it can be used for generalized Boolean functions. Finally, we establishes necessary and sufficient conditions for correlation immunity between the constituent Boolean function components of a generalized Boolean functions and the function itself.