

Title: Group Testing and its Application to Cryptography

Junji Shikata

Dean, Graduate School of Environment and Information Sciences,
Yokohama National University

Abstract: Group testing is a method to detect some special items called defectives among many whole items with a small number of tests than the trivial individual testing for each item. The applications of group testing include screening blood samples for detecting a disease, and detecting clones which have a particular DNA sequence.

In this talk, a mathematical structure for designing group testing will be introduced, and its application to cryptography will also be introduced. The resultant cryptographic technique would be useful to realize efficient communications or data transmissions in an authenticated manner in the network including 5G and B5G in future.