Abstract:
This thesis is focused on bit based division property using three subsets. Firstly, we introduce important definitions such as block cipher, integral attack and conventional division property. Then we define bit based division property using three subsets and prove its propagation rules: copy, AND-compression and XOR-compression. We often use these functions in cryptography, therefore in this thesis we will prove how bit based division property with three subsets propagates after the application of these functions.