

This bachelor thesis describes Correlation attacks on combination generator type stream ciphers. The reader is briefly acquainted with the basic definitions of cryptographic theory which is necessary to understand the text. Afterwards, the thesis describes the original article that presented this type of attack, and which was the inspiration for further improvements and modifications. These improvements are then described in more details, namely the group called "Fast correlation attacks" which are more efficient and fully replaced the original attack. Finally, the thesis describes some modifications of Fast correlation attacks.