1 Stream Ciphers

Carl Schünemann (cas0597), Larysa Bondar (lab7449), Simon Thalmaier (sit7432)

1.1 Weaknesses of LFSRs

1.1.1 Linear complexity of a pseudorandom number

1.1.2 Cracking LFSR: The Berlekamp-Massey algorithm

test [1]

1.2 Combining multiple LFSRs

References

[1] Nigel P. Smart. *Cryptography made simple*. Information security and cryptography. Cham et al.: Springer, 2016. ISBN: 3319219359.