Abstract

The SOBER family ciphers are generally constructed from a linear feedback shift register (LFSR), a non linear filter (NLF) and a form of irregular decimation called stuttering. Our work aims at having a comparative study of the SOBER family of stream ciphers with regard to design philosophies adapted and security aspects.
Reference

-Philip Hawkes, Cameron McDonald, Michael Paddon, Gregory G. Rose, and Miriam Wiggers de Vries, “Primitive Specifications for NLSv2”

Index Terms

Computer Science       Security

Key words

SOBER                LFSR
NLF                  Stuttering