Cryptanalysis of ZUC

Florent Mazelet*[1,2], Léo Perrin[1], Anne Canteaut[1], Aurélien Boeuf[1], and Gaëtan Leurent[1]

[1]Cryptologie symetrique, cryptologie fondee sur les codes et information quantique – Centre Inria de Paris – France

[2]Centre Inria de Paris – Institut National de Recherche en Informatique et en Automatique – France

Résumé

ZUC is a stream cipher used for encryption in 4G and 5G communications which is composed of an LFSR (Linear Feedback Shift Register) over ${F}_{2^{31}-1}$ and an FSM (Final State Machine) over a binary field.

Although the algorithm is widely used, classical attacks on stream ciphers such as fast correlation attacks are difficult to evaluate on it due to its particular structure including operations over different fields. Thus even if correlations exist between the output of the cipher and its internal state, making the link between fields with different characteristics was still left as an open problem.

In this work we find a way to compute the probabilities of propagating masks from a binary field to a non binary field and we give the first key-recovery attack on the keystream generation of ZUC-256 with data and time complexity below 2^{256}.

*Intervenant