Stankovski, Paul; **Hell, Martin**; **Johansson, Thomas**

An efficient state recovery attack on X-FCSR-256. (English) Zbl 1248.94096

Dunkelman, Orr (ed.), Fast software encryption. 16th international workshop, FSE 2009, Leuven, Belgium, February 22–25, 2009. Revised selected papers. Berlin: Springer (ISBN 978-3-642-03316-2/pbk). Lecture Notes in Computer Science 5665, 23-37 (2009).

Summary: We describe a state recovery attack on the X-FCSR-256 stream cipher of total complexity at most $2^{57.6}$. This complexity is achievable by requiring $2^{49.3}$ output blocks with an amortized calculation effort of at most $2^{8.3}$ table lookups per output block using no more than 2^{33} table entries of precomputational storage.

For the entire collection see [Zbl 1168.68003].

MSC:

94A60 Cryptography
94A55 Shift register sequences and sequences over finite alphabets in information and communication theory

Keywords:

stream cipher; FCSR; X-FCSR; cryptanalysis; state recovery

Software:

X-FCSR

Full Text: DOI