Cryptology ePrint Archive: Report 2011/586

TweLEX: A Tweaked Version of the LEX Stream Cipher

Mainack Mondal and Avik Chakraborti and Nilanjan Datta and Debdeep Mukhopadhyay

Abstract: \texttt{LEX} is a stream cipher proposed by Alex Biryukov. It was selected to phase 3 of the eSTREAM competition. \texttt{LEX} is based on the Advanced Encryption Standard {\texttt{AES}) block cipher and uses a methodology called {\em Leak Extraction}, proposed by Biryukov himself. However Dunkelman and Keller show that a key recovery attack exists against \texttt{LEX}. Their attack requires $2^{36.3}$ bytes of keystream produced by the same key and works with a time complexity of 2^{112} operations. In this work we explored \texttt{LEX} further and have shown that under the assumption of a related key model we can obtain 24 secret state bytes with a time complexity of 2^{96} and a data complexity of $2^{54.3}$. Subsequently, we introduce a tweaked version of \texttt{LEX}, called \texttt{TweLEX}, which is shown to resist all known attacks against \texttt{LEX}. Though the throughput of \texttt{TweLEX} is half of \texttt{LEX}, it is still 1.25 times faster than \texttt{AES}, the underlying block cipher. This work attempts to revive the principle of {\em leak extraction} as a simple and elegant method to design stream ciphers.

Category / Keywords: secret-key cryptography / Leak Extraction, Differential cryptanalysis, Tweak, Advanced Encryption Standard

Date: received 28 Oct 2011

Contact author: mainack mondal at gmail com