The Design Trends of Keystream Generator for Stream Cipher for High Immunity Attacks

Saifuldun Mostafa[a] , Hayder Saad[a], Mustafa Musa Jaber[b], Mohammed Hasan Ali[c], Karam Dhafer[a]
[a]Faculty of Computer Science, UKM
[b]Biomedical Computing and Engineering Technologies (BIOCORE) Applied Research Group, Universiti Teknikal Malaysia Melaka (UTeM)
[c]Faculty of Computer Science and Software Engineering, Universiti Malaysia Pahang

ABSTRACT
Due to the latest changes in observing the external network related threats within the stream cipher, it become necessary to address these threats in order to identify the generator suitable for avoiding such threats. In this paper, the researcher addresses the current threats of immunity attacks in the stream cipher. Such attacks are resulted from the correlation within the key stream's multiplexer. The key stream generators are also introduced in order to clarify its working process in avoiding attacks. After all, a comparison of key stream generators are resulted where it can be used as guidelines for other researches in designing key stream generator for high immunity attacks in the cipher.

KEYWORDS: Stream cipher; Immunity attacks; Generator based multiplexer; Key stream

DOI: 10.1007/978-3-319-24584-3_74