清华大学高等研究院

Institute for Advanced Study, Tsinghua University

密码学学术报告 Cryptology Seminars

Title: **On the security of small-state stream ciphers**

Speaker: **Prof. Willi Meier**
(*FHNW University, Switzerland*)

Time: 2018年3月30日（星期五）上午10点

Venue: 清华大学 高等研究院（科学馆）322报告厅

Abstract

Time-memory-data (TMD) tradeoff attacks limit the security level of classical stream ciphers to the birthday bound. Recently, a new field of research has emerged, which searches for so-called small-state stream ciphers that try to overcome this imitation.

In a first part, generic distinguishers for recently proposed small-state stream ciphers are derived whose complexity is significantly smaller than that of exhaustive key search.A new design idea for small-state stream ciphers is presented, which might allow to achieve full security against TMD tradeoff attacks.

In a second part, a fast correlation attack is proposed on Grain-like small-state stream ciphers. This attack is shown to be quite efficient for a recently designed small-state stream cipher.

This is joint work with Matthias Hamann, Matthias Krause and Bin Zhang.