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: **Stream ciphers: old and new directions**

Speaker: **Prof. Willi Meier**
(*University of Applied Sciences and Arts Northwestern Switzerland*)

Time: **2016 年10 月 21 日（周五）上午 10 点**

Venue: **清华大学 高等研究院（科学馆）213 报告厅**

Abstract

Synchronous stream ciphers are used in applications with high throughput requirements or on hardware devices with restricted resources. A review of the development of stream ciphers is given which starts with classical designs and is directed to dedicated stream ciphers in the European NoE eSTREAM project. The history of stream ciphers is rich in new proposals followed by devastating breaks, e.g., by correlation or algebraic attacks. Differential cryptanalysis for chosen plaintext attacks on block ciphers also applies to the initialization mode in stream ciphers, but here, high order differential attacks have proven to be surprisingly successful on constructions based on linear and nonlinear feedback shift registers. The process of designing and cryptanalyzing stream ciphers has not only resulted in building blocks for stream ciphers: Similar components turn out to be useful as well in the design of lightweight block ciphers, hash functions and authenticated encryption. Recent advances in stream ciphers include designs dedicated to application for efficient fully homomorphic encryption, and new designs with short internal state.