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: **Leakage-Resilient Authenticated Encryption and a Sponge Instantiation**

Speaker: **Dr. Chun Guo**
(*Universite catholique de Louvain (UCL), Belgium*)

Time: 2019年4月12日（星期五）下午3点

Venue: 清华大学 高等研究院（科学馆）213报告厅

Abstract

The design of side-channel secure authenticated encryption (AE) is among the most important challenges. To preserve appealing efficiency, we aim at leakage-resilient AE modes supporting "leveled implementations" such that the operations are mainly performed by cheap and weakly protected crypto implementations. To this end, we first propose definitions of leakage-resilient AE schemes. These definitions capture the setting with the leakages of all the computations of an AE scheme, and require security for message encrypted with fresh nonce. This offers various insights on leakage security.

For practical use, we design TETSponge mode from a strongly protected tweakable block cipher and a weakly protected duplex construction. The above is joint work with Olivier Pereira, Thomas Peters, and François-Xavier Standaert from UCL.