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: **Improved Key Recovery Attacks on Reduced-Round AES**

Speaker: **Prof. Adi Shamir**
(*2002 A.M. Turing Award, Weizmann Institute of Science, Israel*)

Time: 2019年4月22日（星期一）上午10点30分

Venue: 清华大学 高等研究院（科学馆）104报告厅

Abstract

Determining the security of AES is a central problem in cryptanalysis, but progress in this area had been slow and only a handful of cryptanalytic techniques led to significant advancements. At Eurocrypt 2017 Grassi et al. presented a novel type of distinguisher for AES-like structures, but so far all the published attacks which were based on this distinguisher were either inferior or comparable to previously known attacks in their complexity. In this talk we combine the technique of Grassi et al. with several other techniques to obtain the best known key recovery attack on 5-round AES in the single-key model, reducing its data, memory and time complexities from about 2^32 to about 2^22. Extending our techniques to 7-round AES, we obtain the best known attacks which use practical amounts of data and memory, breaking the record for such attacks which was obtained 19 years ago by the classical Square attack.