IST AUSTRIA
Institute of Science and Technology

Mathematics and CS Seminar

Securing Cryptography

Maria E. Oswald (U of Bristol)

Host: Krzysztof Pietrzak

Cryptography refers to a set of mathematical techniques that can be used to construct algorithms for privacy, integrity, authenticity, etc. It therefore enables security in many aspects of our online lives. Over the decades, cryptography matured into a rigorous discipline, by mathematically proving security based on clearly formalised adversarial models, strongly inspired by advances in theoretical computer science.In the late 1990s a new threat model emerged that fundamentally challenged our understanding of what suitable adversarial models look like: the emergence of highly practical side channel and fault attacks led to novel adversarial models, and a flurry of papers aiming to solve implementation challenges associated with practical leakage resilience. Despite these academic advances, many real-world implementations of cryptography are still vulnerable to standard side channel attacks. There are several reasons for this: some adversarial models are too strong and therefore constructions too inefficient for practical use, other models are too weak and therefore constructions not useful, but most importantly, many constructions are very difficult to implement securely (leading to a catch-22). Thus, despite all academic advances, implementing cryptography securely is still difficult even for expert developers.Even worse, with the rapid deployment of embedded devices (as part of sensor networks, smart home devices, etc.) many non-expert developers are required to implement or integrate cryptography securely in software (or hardware). To make informed choices regarding the implementation options for (a given set of) cryptographic algorithms, one needs to understand the multitude of attack techniques, the (sometimes) implicit assumptions made for certain constructions, and the access to some facility to conduct leakage attacks. This poses a new interesting avenue for research: how can we support (non-)expert developers in developing secure cryptographic implementations? In this talk I will address several aspects related to this research challenge, thereby implicitly providing a walk-through some of the advances in side channel research.

Tuesday, January 23, 2018 09:00am - 10:00am

IST Austria Campus Mondi Seminar Room 3, Central Building

This invitation is valid as a ticket for the IST Shuttle from and to Heiligenstadt Station. Please find a schedule of the IST Shuttle on our webpage: https://ist.ac.at/en/campus/how-to-get-here/ The IST Shuttle bus is marked IST Shuttle (#142) and has the Institute Logo printed on the side.