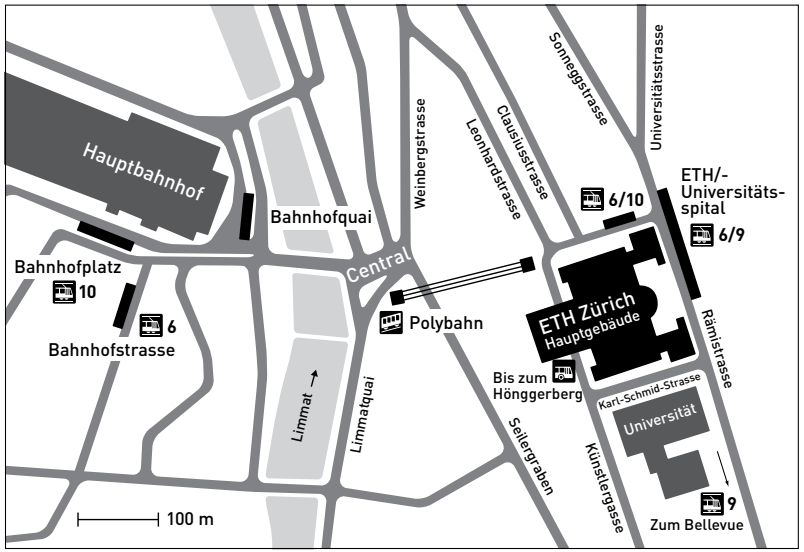


**Location Details**
ETH Zurich, Main Building, Audimax HG F 30, Rämistrasse 101, 8092 Zurich

**How to Reach the Venue**
The Main Building of ETH Zurich can be easily reached by public transportation.
- from Zurich Main Station, take tram no. 6 (direction: Zoo) or tram no. 10 (direction: Zürich Flughafen), tram stop: Universitätsspital/ETH
- from Central, take the Polybahn to the Main Building

**Contact**
ETH Global
www.global.ethz.ch
D-INFK
www.inf.ethz.ch/colloquium

ETH zürich

ETH Global Lecture Series

# Post-Snowden Cryptography

**Monday, 4 May 2015, 16.15 - 17.15**
ETH Zurich, Main Building, Audimax HG F 30,
Rämistrasse 101, 8092 Zurich

**Prof. Adi Shamir**
ETH-ITS;
Weizmann Institute, Israel

Talk jointly organized by
ETH Global and the Distinguished Colloquium of the Department of Computer Science D-INFK

Registration required: **http://bit.ly/1wg0yVY**

ETH Global

Adi Shamir, an Israeli cryptographer and computer scientist and co-winner, with American computer scientists Leonard M. Adleman and Ronald L. Rivest, of the 2002 A.M. Turing Award, the highest honour in computer science, for their "ingenious contribution for making public-key cryptography useful in practice." The three scientists patented their "Cryptographic Communication System and Method," commonly known as RSA encryption, and assigned patent rights to the Massachusetts Institute of Technology (MIT).

Shamir received a bachelor's degree (1973) in mathematics from Tel-Aviv University and a master's degree (1975) in computer science and a doctorate (1977) in computer science from the Weizmann Institute. After a year of postdoctoral work in England at the University of Warwick, Shamir pursued research at MIT (1977–80) before joining the Weizmann Institute (1980– ), where he is the Paul and Marlene Borman Professor of Applied Mathematics.

While at MIT, Shamir met Adleman and Rivest, and in 1977 they produced the first public-key encryption system using digital signatures. Their data-encryption scheme relied on the enormous difficulty of factoring the product of two very large prime numbers, which form a cryptographic key. In 1983 they founded RSA Data Security to pursue commercial applications, which led to the creation of VeriSign, a widely used digital-certification system on the Internet. Millions of people use RSA encryption to secure e-mail and other digital transactions.

Shamir holds more than a dozen patents related to cryptography and computer science. In addition to the Turing Award, Shamir, Adleman, and Rivest were awarded the 2000 Institute of Electrical and Electronics Engineers Koji Kobayashi Computers and Communications Award. Shamir's other awards include the Israel Mathematical Union Erdős Prize in Mathematics (1983), the Association for Computing Machinery Paris Kannellakis Theory and Practice Award (1996), and the Israel Prize in Computer Science (2008).

## Programme

| | |
|---|---|
| 16.15 – 16.20 | **Opening**<br>Prof. Ueli Maurer,<br>Professor of Computer Science, ETH Zurich<br>Information Security and Cryptography Research Group |
| 16.20 – 17.10 | **Post-Snowden Cryptography**<br>Prof. Adi Shamir,<br>ETH-ITS;<br>Weizmann Institute, Israel |
| 17.10 - 17.15 | **Questions & Answers** |
| 17.15 | **Closing** |
| | **Apéro**<br>Foyer Audimax |