**Application**
The application should include:
- Name
- Affiliation (university / company)
- Postal address
- Email address
- Letter of motivation
- short CV

Places are limited. For the selection of the participants the date of the application and the „Letter of motivation“ are relevant, thus early application is recommended.

**Please send your application to Melina Metzig-Lotter:** melina.metzig-lotter@kit.edu.

**Participation fees**
(including: lectures, meals and lodging)
- Bachelor/Master students: 100 Euro
- PhD students: 250 Euro
- others: 350 Euro

There is a very limited amount of travel grants available. In case you want to apply for one, please attach a justification to your application.

**Website**
For further information visit our website:
http://summerschool.iti.kit.edu/

**Partners**

**Editor**
Karlsruhe Institute of Technology (KIT)
Kaiserstr. 12
76131 Karlsruhe
www.kit.edu

www.informatik.kit.edu
Topics
The summer school aims to give an overview of two algorithmically difficult problem classes that are used in public-key cryptography (PKC): computing discrete logarithms and problems in (integer) lattices. Participants will thus learn new developments in an established problem in PKC (dLog-based systems) and in one of the most promising new areas (lattice-based cryptography). Any breakthrough in either of these topics has a major impact on the development of PKC.

For IT security the real implementation with all its side effects is one of the biggest problems. Almost all successful attacks on security systems exploit vulnerabilities in the implementation (software or hardware). An approach that uses coding theory for countermeasures to side-channel attacks covers this topic.

A short overview of the use of cryptography in history and a discussion of current political limits and demands of cryptography will complete the themes of the summer school.

The target audience are Bachelor students (close to finishing their studies), master students, PhD students and interested researchers.

Speakers
The speakers and the (preliminary) titles of their presentations are:

- **Willi Geiselmann, Felix Ulmer**
  Introduction to Cryptography and discrete logarithms in finite groups

- **Sylvain Guilley**
  Complementary Dual Codes for Counter-measures to Side-Channel Attacks

- **Antoine Joux**
  Algorithms to calculate discrete logarithms

- **Vadim Lyubashevsky**
  Public key encryption with lattices,
  Signatures with lattice based cryptography

- **Jörn Müller-Quade**
  Historical and political impact of Cryptography

Venue
The summer school will take place in Bad Herrenalb in the Black Forest some 30 km south of Karlsruhe. The venue is „Haus der Kirche - Evangelische Akademie Baden“ and can be reached from Karlsruhe Main Station (Karlsruhe Hbf) in some 40 minutes by tram and 5 minutes walking.

The accommodation is in single rooms, including shower/WC, desk, internet access. The following meals are included: a grand breakfast buffet, a 3-course menu, coffee with cake and a hot or cold dinner buffet.

The seminar room is equipped with modern technology. To enjoy the evenings there are common rooms, a library and a bar. The area around is perfectly suited for a walk during the breaks.