

---

## - Ph. D. scholarship - "Cryptography"

---

The **Center for Advanced Security Research Darmstadt (CASED)** affiliated to the Department of Computer Science at Technische Universität Darmstadt in Germany offers

### 1 PhD scholarship in Cryptography

starting immediately. The scholarship amounts to 1,468 EUR per month (net) and will be granted for 2 years with the possibility of extension to a third year. The PhD candidate will be working in the Cryptographic Protocols Group (CRYPO) of TU Darmstadt under supervision of Prof. Mark Manulis and will be inscribed into the 3-year doctoral program at CASED. The PhD candidate will be expected to do active and internationally visible research on modern topics of public-key cryptography and provable security, especially in the area of digital signatures and multi-party protocols.

The PhD position offers space for own creativity and research work will be conducted in close international cooperation with world-wide leading research institutions. Successful candidates must hold an outstanding M.Sc. degree (or equivalent) from the university study of Mathematics, Computer Science, Information Security, or similar, obtained within the last two years. The topic of the master thesis should ideally have relevance to cryptography or information security. Applications of students that are about to finish their master thesis will be accepted as well. Amongst further requirements are excellent skills in English language and basic knowledge in computer networks and programming.

CASED is an IT Security research center at TU Darmstadt in cooperation with the Fraunhofer Institute for Secure Information Technology (SIT) and the University of Applied Sciences Darmstadt (h\_da). CASED aims at having a significantly higher proportion of female scientists compared to the average German research institutions and encourages applications of female postgraduate students.

Applicants are kindly requested to send their applications by e-mail to [mark@manulis.eu](mailto:mark@manulis.eu) and [advisory\\_board\\_of\\_study\\_affairs@cased.de](mailto:advisory_board_of_study_affairs@cased.de) (in CC).

#### Applications must include:

- a letter of application,
- a CV,
- a statement of motivation (incl. the description of prior activities with relevance to cryptography or information security),
- academic transcripts (incl. table of grades),
- and two references or letters of recommendation.

Applications will be processed until the position is filled

#### Links

- Cryptographic Protocols Group, <http://www.cryo.informatik.tu-darmstadt.de/cryo/>
- CASED, [www.cased.de](http://www.cased.de)
- TU Darmstadt, [www.tu-darmstadt.de](http://www.tu-darmstadt.de)