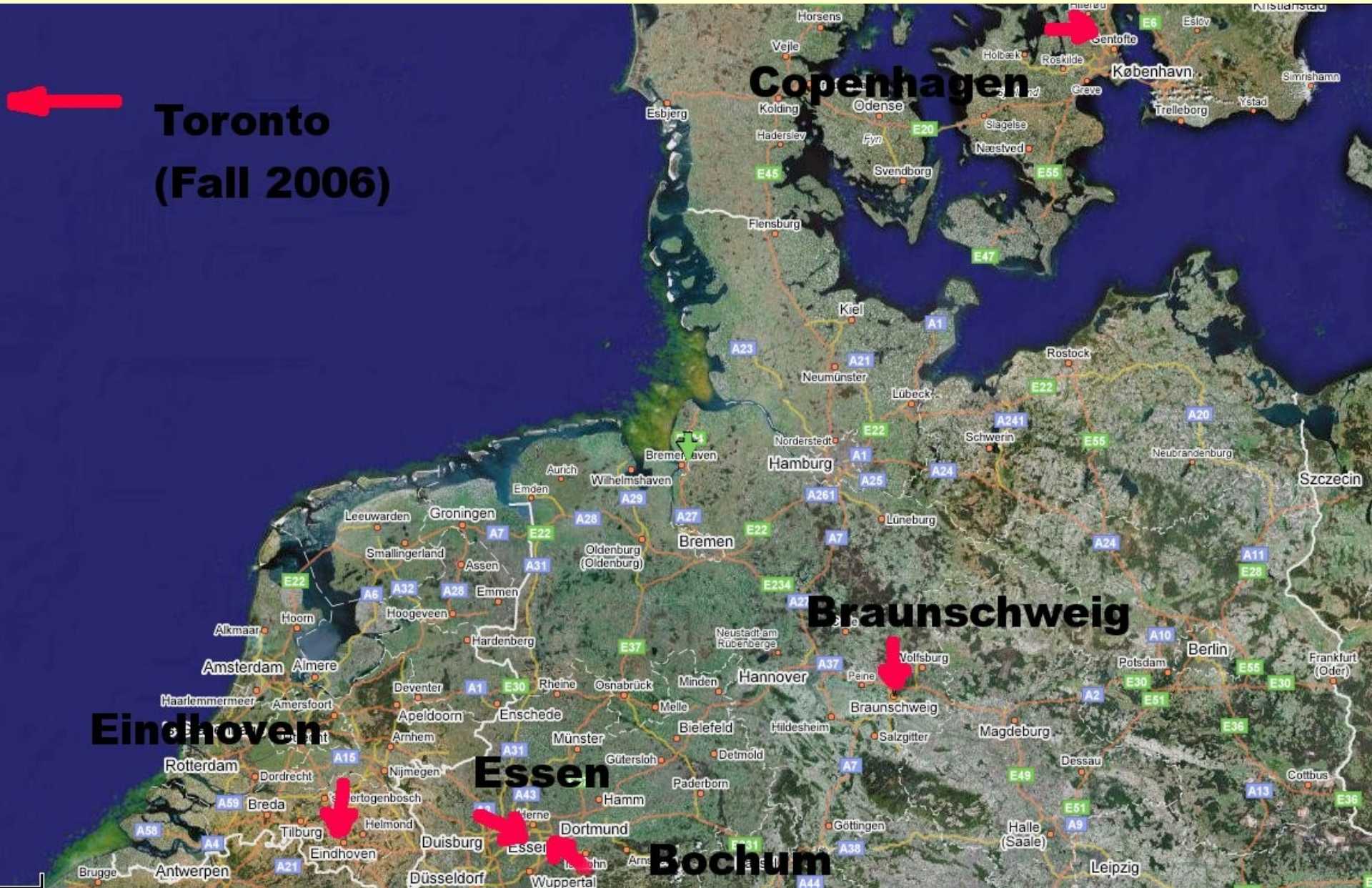


Tanja Lange

**Full Professor
Coding and Cryptology
HG 9.88
Tel.: 4764**

www.hyperelliptic.org/tanja

Stations of a journey:



Toronto
(Fall 2006)

Copenhagen

Braunschweig

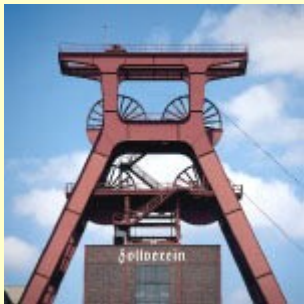
Eindhoven

Essen

Bochum

CV data I:

- Born in Bad Gandersheim, Germany
- Diploma (Mathematics) and Staatsexamen (Mathematics and Physics) at TU Braunschweig



- PhD (Mathematics) in Essen under supervision of Gerhard Frey

CV data II:

- Research assistant at the Ruhr-University Bochum; part of the Horst-Görtz Institute for IT-security



- Associate professor at the Technical University of Denmark (Lyngby, a bit north of Copenhagen)



- Fields Institute Toronto – Fall '06 Thematic Program on Cryptography

Research area: Cryptography

- Construction and analysis of primitives for public key systems
- Side-channel attacks and countermeasures

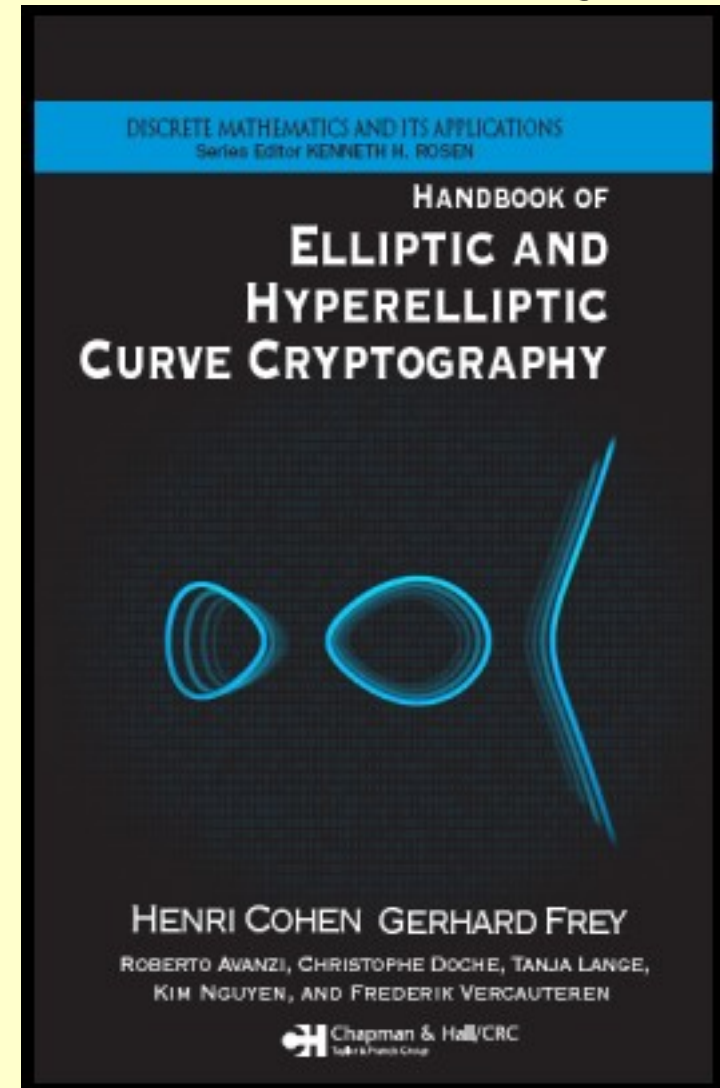


- Efficient implementation of cryptographic primitives
- Protocols for secure and efficient use of primitives

Research area: Computational Number Theory

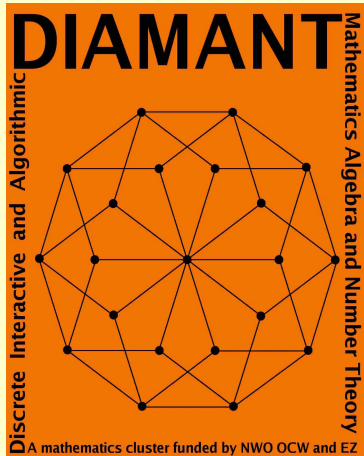
- strong interaction with research in cryptology
- elliptic and hyperelliptic curves over finite fields
- pairing computation
- finite fields and applications
- factorization of polynomials
- character sums

Tanja Lange – TU Eindhoven



Projects and collaborations

- Management board of ECRYPT
(European Network of Excellence
in Cryptology)



- Member of DIAMANT (Discrete
Interactive and Algorithmic
Mathematics Algebra and
Number Theory)

- Close collaborations with
Bochum, Bristol, Chicago, Copenhagen,
Essen, Linz, London, Sydney