Discrete Mathematics

Technische Universiteit
Eindhoven
University of Technology

Where innovation starts

Discrete Mathematics

- Coding Theory and Cryptology
  www.win.tue.nl/cc
- Cryptographic Implementations
  eindhoven.cr.yp.to
- Discrete Algebra and Geometry
  www.win.tue.nl/.../discrete-algebra-and-geometry
- Combinatorial Optimization
  www.win.tue.nl/.../combinatorial-optimization-co

Coding Theory and Cryptology

Coding Theory

- error correcting codes
- information theory
- algebra, combinatorics, geometry, statistics …

Cryptology

- secret messages, hash functions
- digital signatures, certificates
- secure multi-party computation, protocols
- internet auctions, electronic elections
- algorithms, number theory, …

Coding Theory and Cryptology

Tanja Lange

crypto on (hyper)elliptic curves

code based crypto

www.hyperelliptic.org/tanja

Berry Schoenmakers

cryptographic protocols

multi-party computation

www.win.tue.nl/~berry

TU/e Technische Universiteit Eindhoven University of Technology

Coding Theory and Cryptology

Ruud Pellikaan

algebraic geometry codes

code based crypto

www.win.tue.nl/~ruudp

Benne de Weger

lattice based crypto

hash functions

algorithmic number theory

www.win.tue.nl/~bdeweger

TU/e Technische Universiteit Eindhoven University of Technology

Coding Theory and Cryptology

Ruben Niederhagen

parallel architectures

http://polycephaly.org

Meilof Veeningen

secure multi-party computation

http://meilof.home.fmf.nl

TU/e Technische Universiteit Eindhoven University of Technology

Coding Theory and Cryptology

Thijs Laarhoven

lattice based crypto

hash functions

http://www.thijs.com

Jan-Jaap Oosterwijk

digital watermarks

http://www.win.tue.nl/~joosterw

TU/e Technische Universiteit Eindhoven University of Technology

Coding Theory and Cryptology

Putranto Hadi Utomo

Binary Puzzles

Constrained Arrays

http://putranto.staff.uns.ac.id/

TU/e Technische Universiteit Eindhoven University of Technology

Cryptographic Implementations

Dan Bernstein

cryptographic implementations

cr.yp.to/djb.html

cryptographically protect
every Internet packet against
espionage, corruption, and sabotage

Cryptographic Implementations

Andreas Hulsing

hash-based signature schemes

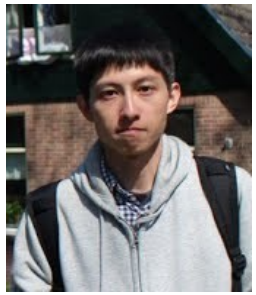
http://huelsing.wordpress.com

Tony Chou

fast implementations

code-based cryptosystems

sites.google.com/a/crypto.tw/blueprint



TU/e Technische Universiteit Eindhoven University of Technology

Cryptographic Implementations

Chitchanok Chuengsatiansup

elliptic and hyperelliptic curve cryptography

pairing-based cryptography

side-channel analysis

https://sites.google.com/site/cchuengs

Christine van Vredendaal

algorithmic cryptanalysis

http://scarecryptow.org

TU/e Technische Universiteit Eindhoven University of Technology

Security

Sandro Etalle

www.win.tue.nl/~setalle

network intrusion detection

protection of industrial control systems

access control and trust management

usage control and privacy protection

verification of security protocols.

TU/e Technische Universiteit Eindhoven University of Technology

Security

Milan Petkovic

win.tue.nl/~petkovic

Information security

Secure data management

Boris Skoric

security1.win.tue.nl/~bskoric

Secure key storage

Anti-counterfeiting

Institute: EIPSI - EI/Ψ

EIPSI www.win.tue.nl/eipsi/

- Coding Theory and Cryptology
  www.win.tue.nl/cc
- Cryptographic Implementations
  eindhoven.cr.yp.to
- Security
  www.win.tue.nl/sec

The Kerckhoffs Institute

The Kerckhoffs Institute for Computer Security

www.kerckhoffs-institute.org/

The institute is a collaboration between:

- University of Twente
- Eindhoven University of Technology
- Radboud University Nijmegen

Offers a 2-year master track in computer security as part of a computer science master programme

MasterMath

Dutch Master's Degree Program in Mathematics

www.mastermath.nl/

Technische Universiteit
Eindhoven
University of Technology

Brochures and weblinks

1) Graduate Programs

https://www.tue.nl/en/education/tue-graduate-school/graduate-programs/

2) Overview Academic Programs

http://flippingbooks.tue.nl//internet/folder-internationale-werving/index.html#

3) Industrial and Applied Mathematics

https://www.tue.nl/en/education/tue-graduate-school/graduate-programs/industrial-and-applied-mathematics-graduate-program/

4) PhD program Industrial and Applied Mathematics

https://www.tue.nl/en/education/tue-graduate-school/graduate-programs/industrial-and-applied-mathematics-graduate-program/phd-program-industrial-and-applied-mathematics/