**Core Team**
- Bernhard Esslinger
- Dominik Schadow
- Matthias Walchert
- Simon Leischhig

...and many plug-in developers...

**Features**
- e-learning
- Modern user interface
- Open source
- Platform independent
- Extensible through plug-ins
- Java
- Eclipse
- Rich Client Platform RCP
- JCA/JCE

**Crypto Algorithms**
- Classes and modern symmetric encryption
- Hash, MAC, signature
- PRNG
- Asymmetric encryption
- Cryptanalysis
- Visualizations (extended Euclidean, Kleptography, multipartite key exchange, CRT, ...)

**Crypto Provider**
- BouncyCastle
  - Cryptographic algorithms
- FlexiProvider
  - Cryptographic algorithms
  - Keystore

**Project History**
- 1998: CrypTool project started
- 2000: Available as freeware
- 2003: Available as open source
- 2007: JCryptool project started
- 2010: JCryptool 1.0

**PostQuantum**
- Niederreiter
- McEliece
- McEliece-Fujisaki
- McEliece-Kobayashi
- McEliece-Patarin
- Niederreiter-CFS
- Merkle-OTS
- CMSS
- GMSS

**Samples of built-in visualizations**

**ECC Demonstration**
- Choose points
- Addition
- Scalar multiplication

**Games**
- Number Shark

**Shamir’s Secret Sharing**
- Numerical and graphical mode
- Arbitrary number of shares

---

**www.cryptool.org**

**PQCrypto 2010**
Darmstadt, Germany
May 25 - 28, 2010