Universität Bremen*

Recommendation to Protect Your Data in the Future

Prof. Dr.-Ing. Tim Güneysu

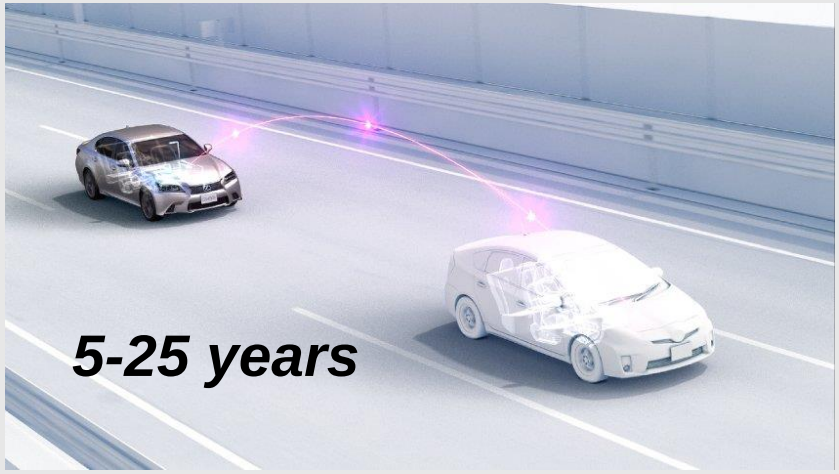
Arbeitsgruppe Technische Informatik / IT-Sicherheit (CEITS)

LEARNTEC – Karlsruhe – 27.01.2016

*EXZELLENT.

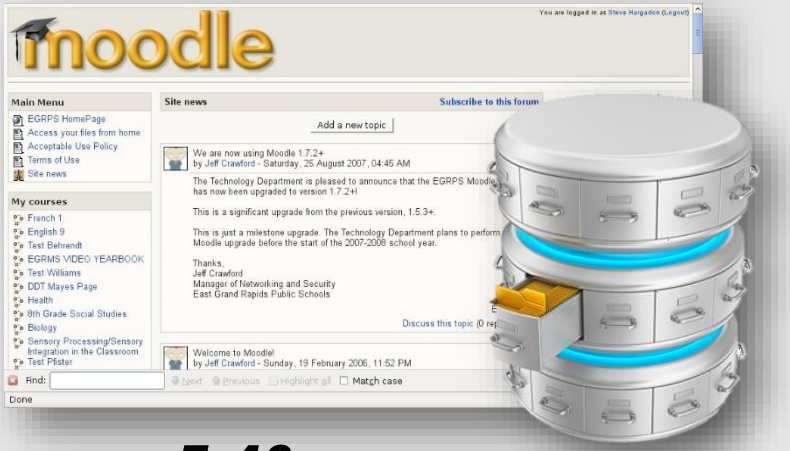
Long-Term Security in the Real World

- Most IT applications have a **long-term security requirements for their data**
- Some of the deployed systems are strictly constrained in memory and computational power



> 8 years

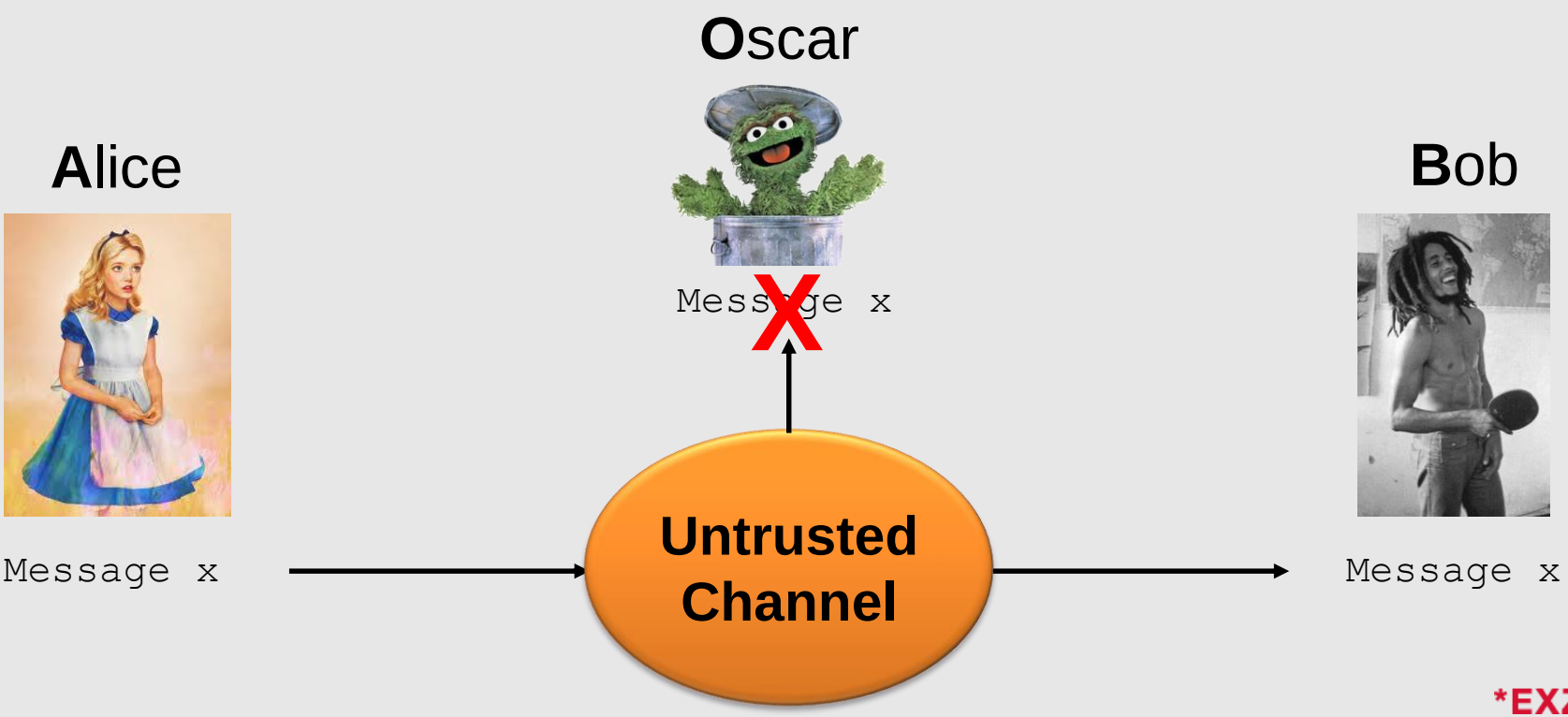
10 years



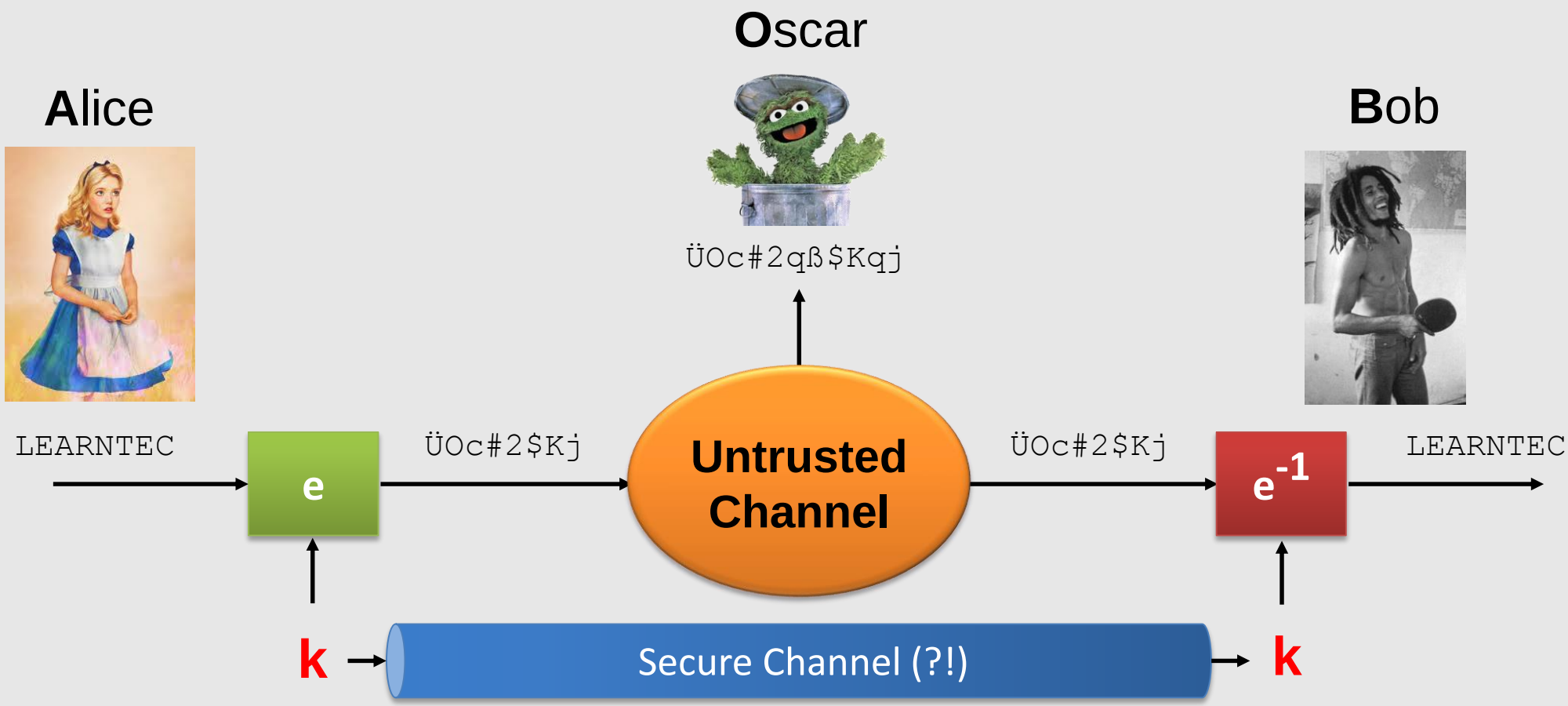
5-40 years

Basics on Cryptography

- Fundamentals of security are founded on **cryptography**
- Cryptography provides a large variety of security services (such as confidentiality, authentication, integrity, anonymity,…)
- **This talk**: Towards long-term secure encryption systems



Introduction to Symmetric Cryptography

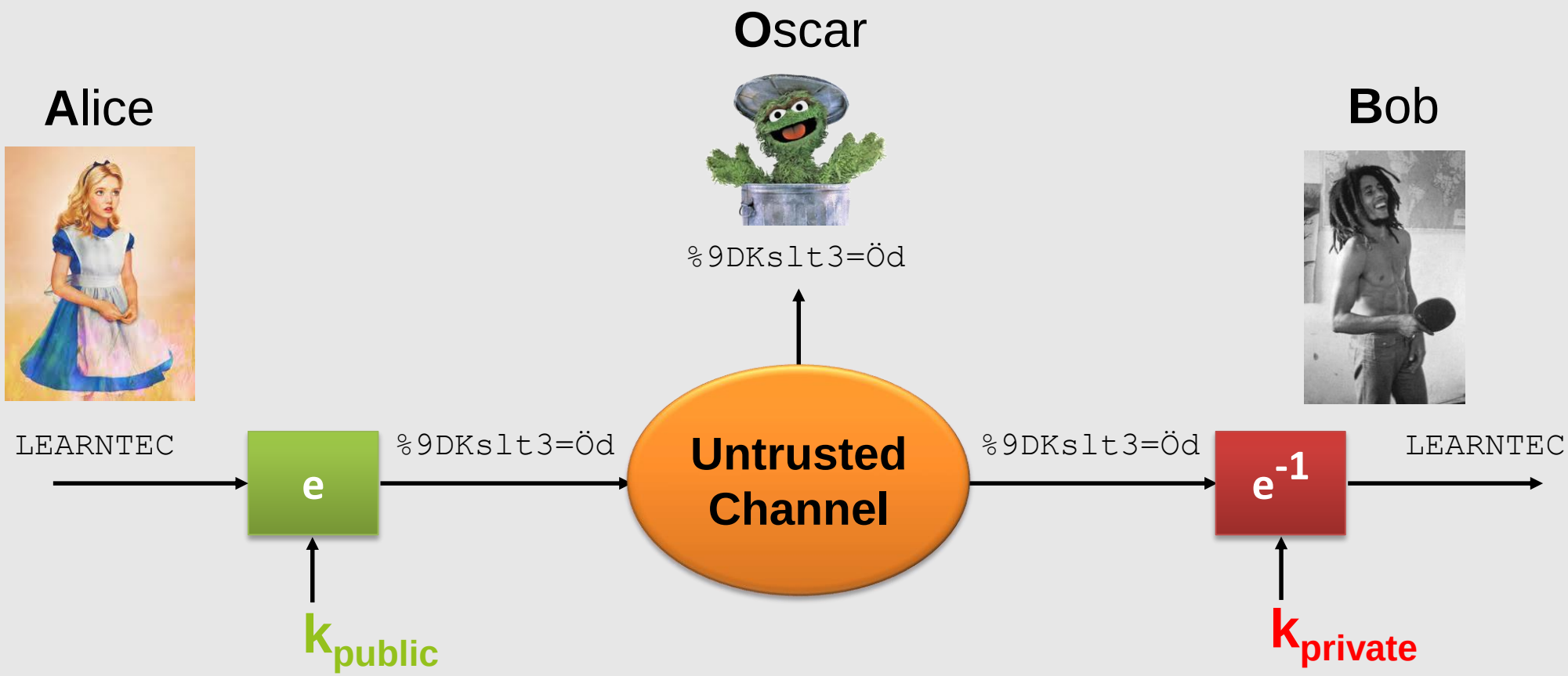


Common problem:

– How can Alice and Bob securely exchange the shared secret **k** prior to communication?

Asymmetric Cryptography

Alternative: Use asymmetric encryption with two key shares (k_{public} , $k_{private}$)



- **Fundamental challenge:**
  - Function *e* must be efficient for evaluation in both directions for all key shares (k_{public} , $k_{private}$)
  - Inverting *e* is hard if $k_{private}$ is not present

Examples: The Case of RSA and ElGamal

RSA Cryptosystem

Setup/Parameters
Choose $n = p \cdot q$ with p,q prime
Pick e with $\gcd(e, \varphi(N)) = 1$ and
with $e \cdot d = 1 \; mod \; \varphi(N)$
Public key: $k_{public} = (n, e)$
Private key: $k_{private} = d$

RSA encryption for message m ∈ Z_n^*
Encrypt: $\boldsymbol{c} = \boldsymbol{m}^{\boldsymbol{e}}$ mod n
Decrypt: $\boldsymbol{m} = \boldsymbol{c}^{\boldsymbol{d}}$ mod n

Integer Factorization Problem

ElGamal Cryptosystem

Setup/Parameters
Given p prime and generator $g \in Z_p^*$
Pick random $a \in Z_{p-1}/\{0,1\}$ and
compute $b = g^a \; mod \; p$
Public key: $k_{public} = (b, p)$
Private key: $k_{private} = a$

RSA encryption for message m ∈ Z_n^*
Encrypt: Pick random $i \in Z_{p-1}/\{0,1\}$ and
compute $t = g^i \; mod \; p$
Compute $k = b^i \; mod \; p$
Finally: $\boldsymbol{c} = \boldsymbol{m} \cdot \boldsymbol{k}$ mod n
Decrypt: Compute $k = t^a \; mod \; p$
Finally $\boldsymbol{c} = \boldsymbol{m} \cdot \boldsymbol{k}^{-1}$ mod n

Discrete Logarithm Problem

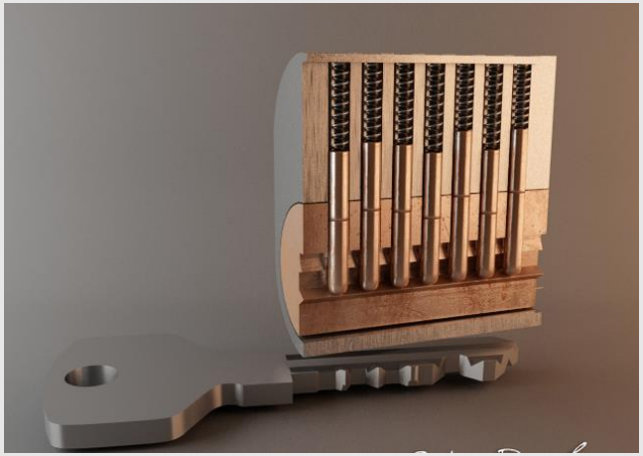
Security of Practical Cryptographic Primitives

- Cryptosystems must combine **security** and **efficiency**

- Embedded devices usually deploy **standardized cryptography**
  - Symmetric encryption: *Advanced Encryption Standard*
  - Asymmetric encryption: *RSA (Factorization Problem), ElGamal or Elliptic Curve Cryptography (Discrete Logarithm Problem)*

- **No proofs for the hardness of any of these cryptographic systems**

- **Thus: Select security parameters to resist best known cryptanalytic attack(s)**



Best Attacks on Standard Cryptosystems

- **Attacks on symmetric cryptosystems**
  - Modern ciphers employ well-understood principles
  - Best attacks on solid symmetric ciphers is exhaustive key search
  - Rather easy to tweak for long-term security by scaling key sizes

- **Attacks on asymmetric cryptosystems**
  - Almost all cryptosystems rely on the two problems
    - Factorization problem (RSA)
    - Discrete Logarithm problem (DLOG)
  - Best known attacks with subexponential complexity
    - General Number Field Sieve (on RSA)
    - Index Calculus (on DLOG)
  - Still, long-term security parameters with **no real security guarantee**

Key Size Recommendations

- Security parameters assuming ***today's*** algorithmic knowledge and computing capabilities of an advanced attacker

Security (bits) (symmetric)	RSA	DLOG		EC
		field size	subfield	
48	480	480	96	96
56	640	640	112	112
64	816	816	128	128
80	1248	1248	160	160
112	2432	2432	224	224
128	3248	3248	256	256
160	5312	5312	320	320
192	7936	7936	384	384
256	15424	15424	512	512

Source: ECRYPT II Yearly Key Size Report 2011-2012

Public-Key Cryptography and Long-Term Security

- **All currently deployed asymmetric cryptosystems** (RSA, ElGamal, ECC) **will become obsolete as soon as powerful quantum computers exist** (cf. Shor 1994)

- Note that **RSA & DLOG cryptosystems are closely related**

- Even without quantum computers, **diversity of cryptosystems** in the cryptographic basket is essential

Alternatives for Public-Key Cryptography (I)

- **Solutions** for alternative public-key cryptosystems are already required today
- Ideally, with security reductions based on **NP-hard problems**
- **No polytime attacks on quantum computers (such as Grover‘s/Shor‘s alg.)**
- **Efficiency in implementations** comparable to currently deployed systems

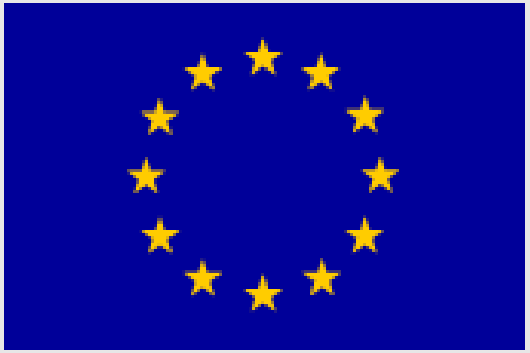
Alternatives for Public-Key Cryptography (II)

- **Four main branches of post-quantum crypto:**
  - Code-based
  - Hash-based
  - Multivariate-quadratic
  - Lattice-based
- **Support public-key encryption and/or signature schemes**

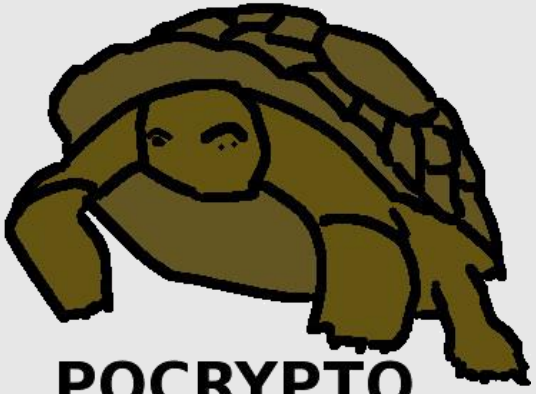
EU Horizon 2020:
Post-Quantum Cryptography (PQCRYPTO)

Universität Bremen*

- **Project Goals**
  - Identification and (re-)design of alternative cryptosystems resisting attacks from quantum computers
  - Development of efficient implementations as drop-in replacements for today's cryptography



- **Project Timeframe**
  - March 2015 – Feb 2018

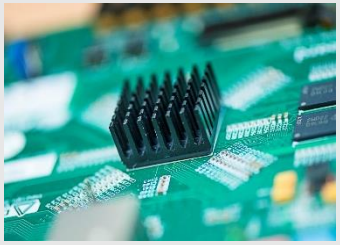


PQCRYPTO
ICT-645622

- **Project Consortium**
  - Coordinator: TU Eindhoven (Tanja Lange)
  - 11 Partners, 1 Associated (Taiwan)

Project Work Packages

- **WP1: Post-quantum cryptography for small devices**



  - Leader: Tim Güneysu (Uni Bremen)
  - Co-leader: Peter Schwabe (RU Nijmegen)

- **WP2: Post-quantum cryptography for the Internet**

  - Leader: Daniel J. Bernstein (TU Eindhoven)
  - Co-leader: Bart Preneel (KU Leuven)

- **WP3: Post-quantum cryptography for the cloud**

  - Leader: Nicolas Sendrier (INRIA Paris)
  - Co-leader: Lars Knudsen (DTU Kopenhagen)

PQCRYPTO: Partners

TU/e technische universiteit eindhoven

University of Haifa

DTU Danmarks Tekniske Universitet

Inria INVENTEURS DU MONDE NUMÉRIQUE

KU LEUVEN

Radboud Universiteit

50 Jahre RUB

TECHNISCHE UNIVERSITÄT DARMSTADT

BUNDES DRUCKEREI

NXP

ACADEMIA SINICA

Initial Recommendations (as of March 2015)

- **Conservative recommendations**
  - Symmetric cryptography
    - *Block ciphers*: AES with 256-bit key [1]
    - *Stream ciphers*: Salsa20 with 256-bit key [2]
  - Asymmetric cryptography
    - *Code-based encryption*:
      McEliece Encryption with binary Goppa codes using length n = 6960, dimension k = 5413 and adding t = 119 errors [3]
    - *Hash-based digital signatures*:
      XMSS with 256-bit parameter set [4] or SPHINCS-256 [5]

- **Further more experimental choices are under investigation**

References

[1] Joan Daemen and Vincent Rijmen. The Design of Rijndael: AES - The Advanced Encryption Standard. Information Security and Cryptography. Springer, 2002

[2] Daniel J. Bernstein. The Salsa20 Family of Stream Ciphers. In Matthew J. B. Robshaw and Olivier Billet, editors, New Stream Cipher Designs - The eSTREAM Finalists, volume 4986 of Lecture Notes in Computer Science, pages 84–97. Springer, 2008.

[3] Daniel J. Bernstein, Tung Chou, and Peter Schwabe. McBits: Fast Constant-Time CodeBased Cryptography. In Guido Bertoni and Jean-Sebastien Coron, editors, Cryptographic Hardware and Embedded Systems - CHES 2013 - 15th International Workshop, Santa Barbara, CA, USA, August 20-23, 2013. Proceedings, volume 8086 of Lecture Notes in Computer Science, pages 250–272. Springer, 2013.

[4] Johannes A. Buchmann, Erik Dahmen, and Andreas Hülsing. XMSS - A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions. In BoYin Yang, editor, Post-Quantum Cryptography - 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29 - December 2, 2011. Proceedings, volume 7071 of Lecture Notes in Computer Science, pages 117–129. Springer, 2011.

[5] Daniel J. Bernstein, Daira Hopwood, Andreas Hülsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Michael Schneider, Peter Schwabe, and Zooko WilcoxO'Hearn. SPHINCS: Practical Stateless Hash-Based Signatures. In Elisabeth Oswald and Marc Fischlin, editors, Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I, volume 9056 of Lecture Notes in Computer Science, pages 368–397. Springer, 2015.

Universität Bremen*

Recommendation to Protect Your Data in the Future

Prof. Dr.-Ing. Tim Güneysu

Arbeitsgruppe Technische Informatik / IT-Sicherheit (CEITS)

LEARNTEC – Karlsruhe – 27.01.2016

*EXZELLENT.