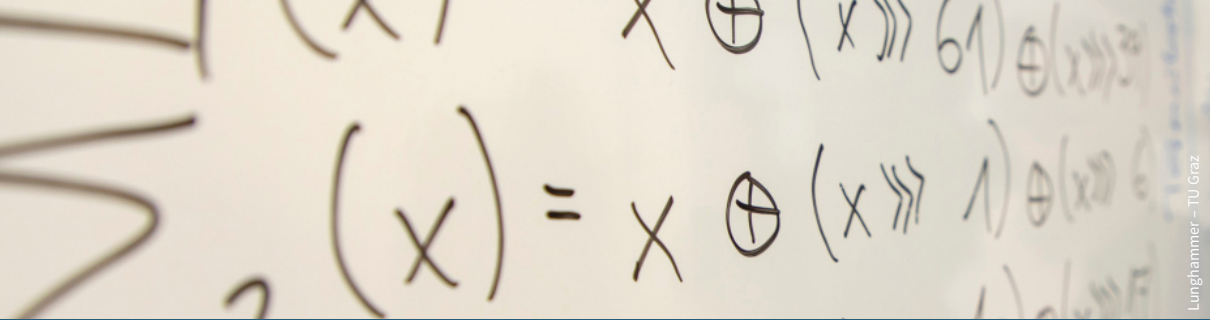

Applied Cryptography 2

Maria Eichlseder
Daniel Kales
Christian Rechberger
Markus Schofnegger

Summer Term 2020

Conclusion

Cryptanalysis

…or how to scale your cipher

- Asymmetric cryptanalysis:
  - RSA: Factoring (L1)
  - PQ schemes etc.: Lattice reduction (L4) and other ingredients (S3)
- Symmetric cryptanalysis:
  - Differential (L5, L7, L10), linear (L6, L7), algebraic (L8, S5) attacks
  - (In)Security of modes (L9, S2)

Cryptographic Designs

…or what your cipher can do

- Advanced security notions & ingredients:
  - Multi-Party Computation (L2, L3)
  - Homomorphic Encryption (S4)
  - Post-Quantum Crypto (S3)
- Security in practice:
  - Password Hashing (S1)

End-of-term reminders

Exercises (KU)

KU Interviews (“Abgabegespräche”)

- Ongoing: today and more slots on Thursday 9 July
- Make sure to contact us if these are unsuitable for you

KU Evaluation

- Open tomorrow until Thursday 9 July
- Please give us feedback!
- How hard / interesting / time-consuming was each task?
- How did Corona affect your experience?

Lecture (VO)

VO Exam

- Thursday 2 July: written “Corona-style” exam
- Or later: ask for a [virtual|real] oral exam date

Exam questions:

- Choose 4 out of 5 questions
- Updated list of questions is (soon) online

$\geq 87.5\,\%$	1
$\geq 75.0\,\%$	2
$\geq 62.5\,\%$	3
$\geq 50.0\,\%$	4
else	5

VO Evaluation

- Open now until Thursday 9 July

You might also like…

Crypto-Related Lectures

New curricula and lecture names next winter term!

- Prev course, Applied Crypto $\rightarrow$ Cryptography
- This course, Applied Crypto 2 $\rightarrow$ Cryptanalysis
- IT Security $\rightarrow$ Privacy Enhancing Technologies
- AK ITS 2 (Modern Public Key Cryptography) $\rightarrow$ Selected Topics in Cryptography and Privacy
- AK ITS 2 (Mathematical Background of Cryptography) $\rightarrow$ Seminar Cryptology and Privacy

Master's thesis and projects

- Cryptanalysis of Lightweight Ciphers (NIST Competition)
- Post-Quantum Oblivious Transfer
- Privacy-Preserving Data Analysis
- Tools for Cryptanalysis
- Finding Optimal Attacks on GGM Trees
- Attack or Protect Cryptographic Implementations against Physical Attacks
- Computation on Encrypted Education Data
- …

+ many more security-related topics – ask us!

https://www.iaik.tugraz.at/teaching/master-thesis/

Your questions?