

Theory of Efficient Algorithms



Prof. Dr. Peter Kling – Universität Hamburg

The Team

Research Group TEA

Peter Kling
(Head of Group)



G-229

Katrin Köster
(Team Assistant)



G-218

Focus: Design & Analysis of Algorithms

- Distributed Systems
- Online Computation
- Resource Management

Christiane Frede



G-209

Christoph Damerius

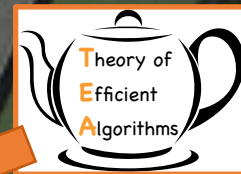


G-226

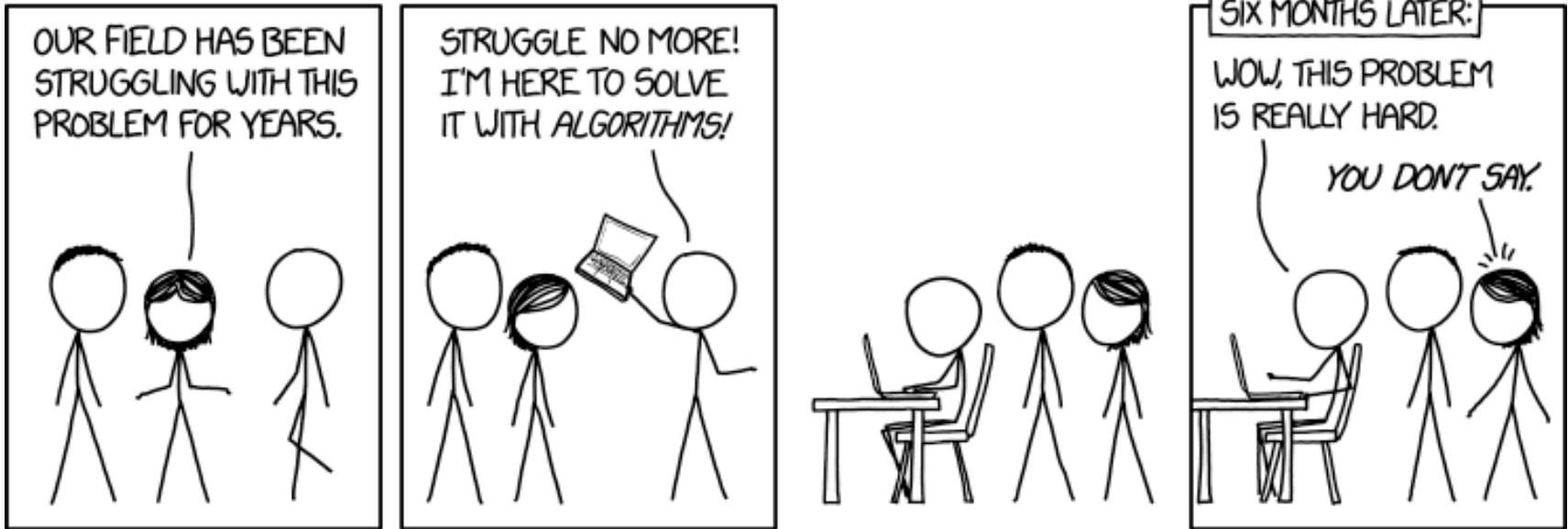
Florian Schneider



G-226



Theory of Efficient Algorithms



Why is the problem hard?

How hard is the problem?

What part of the problem is hard?

Can we solve it anyway?

Teaching

Teaching Overview

Winter Term

InfM-Kryp: Cryptography

Wahlpflichtbereich
Theorie

Summer Term

InfM-MDAE: Methods of Algorithm Design

Wahlpflichtbereich
Theorie

Always

Master's Thesis

talk to me

Cryptography

Module InfM-Kryp

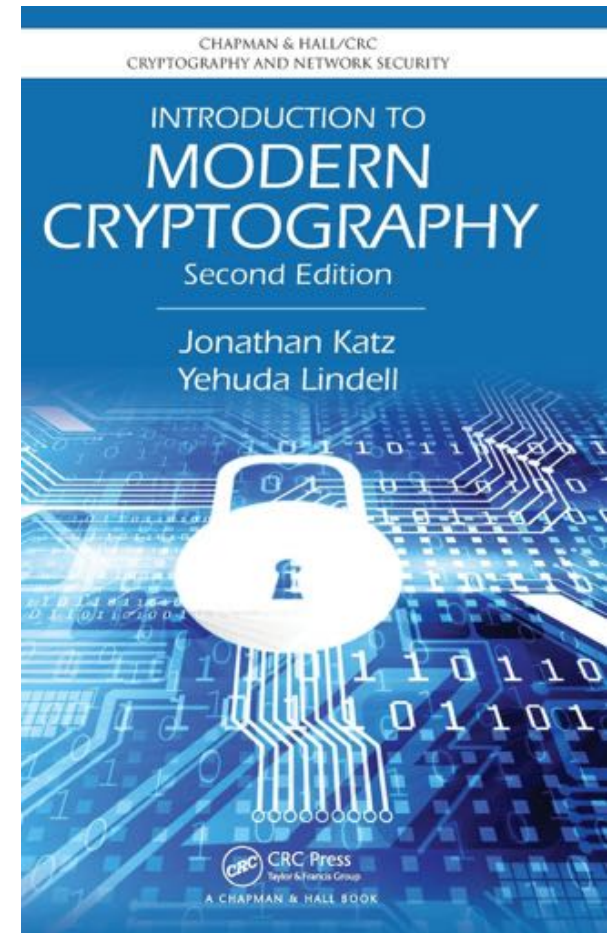
- (Why) Is today's cryptography safe?
- **mathematical** foundations to understand cryptographic protocols
- How to quantify cryptographic security?

Lecture

- definitions + theorems + proofs
- (black-/white-) board + slides
- integrated exercises

Seminar

- block and/or running



Cryptography

Module InfM-Kryp

Substitution Cipher

(Mono-alphabetic)

- key $k \in \mathcal{K}$ with

$\mathcal{K} = \{k \mid k: \{0,1, \dots, 25\} \rightarrow \{0,1, \dots, 25\} \text{ is a permutation}\}$

- example:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
H	Z	L	K	J	I	O	F	R	N	E	G	B	T	X	P	S	D	A	Y	Q	W	C	V	M	U

 $|\mathcal{K}| = 26! \approx 2^{88}$

Gen:

- $k \leftarrow U(\mathcal{K})$

Enc: $m = m_1 m_2 \dots \in \mathcal{M} = \{0,1, \dots, 25\}^*$

- $\text{Enc}_k(m) = c_1 c_2 \dots$, where $c_i = k(m_i)$

Dec: $c = c_1 c_2 \dots \in \mathcal{C} = \{0,1, \dots, 25\}^*$

- $\text{Dec}_k(c) = m_1 m_2 \dots$, where $m_i = k^{-1}(c_i)$

25

Breaking the Substitution Cipher

Warm-up: an improved attack on the Shift Cipher

Decrypt!

ZYDLEFCOLJSPLEPESCZFRSZYPATP
 NPZQNSZSNZWLEPNLVPZYPTNPNC
 PLXNZYPZYPATNVWPZYPDWTNPZ
 QDHTDDNSPPDPZYPDWTNPZQDL
 WLXTZYPWZWWTAZAZYPATPNPZQ
 NSPCCJATPZYPDLFLRPZYPNFANL
 VPLYOZYPDWTNPZQHLEPCXPWZY

26

Frequency Analysis

English-language Letter Frequencies (in %)

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
8.2	1.5	2.8	4.3	12.7	2.2	2.0	6.1	7.0	0.2	0.8	4.2	2.6	6.7	1.5	1.9	0.1	6.0	6.3	9.1	2.8	1.0	2.4	0.2	10	0.1

Ciphertext Letter Frequencies

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
10.1	0	3.25	0.15	2.79	2.28	0	1.12	0	1.12	0	7.26	0	8.94	1.12	16.99	2.79	1.12	3.25	0.15	0	1.68	5.59	1.68	7.81	12.85

Distance via Sum of Squares

$$\sum_{i=0}^{25} p_i^2 \approx 0.06$$

Compute for $k \in \{0,1, \dots, 25\}$:

$$\Delta(k) = \left| \sum_{i=0}^{25} p_i \cdot q_{(i+k) \bmod 26} - \sum_{i=0}^{25} p_i^2 \right|$$

27

Cryptography

Module InfM-Kryp

Proof Theorem 3.6 (1/3)

- let $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ denote Construction 3.2
- let $\tilde{\Pi} = (\tilde{\text{Gen}}, \tilde{\text{Enc}}, \tilde{\text{Dec}})$ denote the scheme that is as Π but uses a truly random function $f \sim U(\text{Func}_n)$ instead of F_k
- note that $\tilde{\Pi}$ is not efficient
- fix an arbitrary PPT adversary \mathcal{A} and let $q(n)$ be an upper bound on the number of queries $\mathcal{A}(1^n)$ makes to its encryption oracle
- \mathcal{A} runs in polynomial time $\Rightarrow q(n)$ bounded by a polynomial
- **Proof Step 1:** We show that there is a negligible function negl' such that

$$\left| \Pr \left[\text{PrivK}_{\mathcal{A}, \Pi}^{\text{cpa}}(n) = 1 \right] - \Pr \left[\text{PrivK}_{\mathcal{A}, \tilde{\Pi}}^{\text{cpa}}(n) = 1 \right] \right| \leq \text{negl}'(n).$$

- **Proof Step 2:** We show that

$$\Pr \left[\text{PrivK}_{\mathcal{A}, \tilde{\Pi}}^{\text{cpa}}(n) = 1 \right] \leq \frac{1}{2} + \frac{q(n)}{2^n}.$$

- **Together**

$$\Pr \left[\text{PrivK}_{\mathcal{A}, \Pi}^{\text{cpa}}(n) = 1 \right] \leq \Pr \left[\text{PrivK}_{\mathcal{A}, \tilde{\Pi}}^{\text{cpa}}(n) = 1 \right] + \text{negl}'(n)$$

$$\leq \frac{1}{2} + \frac{q(n)}{2^n} + \text{negl}'(n) = \frac{1}{2} + \text{negl}(n). \quad \rightarrow \text{done}$$

An ECB Example from Wikipedia



Original



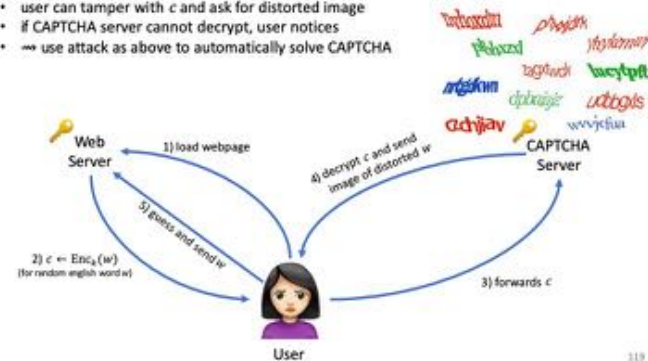
ECB Encryption



secure block mode

Is there a realistic setting for such an attack? CAPTCHAs!

- CAPTCHA server acts as padding-oracle
- user can tamper with c and ask for distorted image
- if CAPTCHA server cannot decrypt, user notices
- \Rightarrow use attack as above to automatically solve CAPTCHA



Methods of Algorithm Design

Module InfM-MDAE

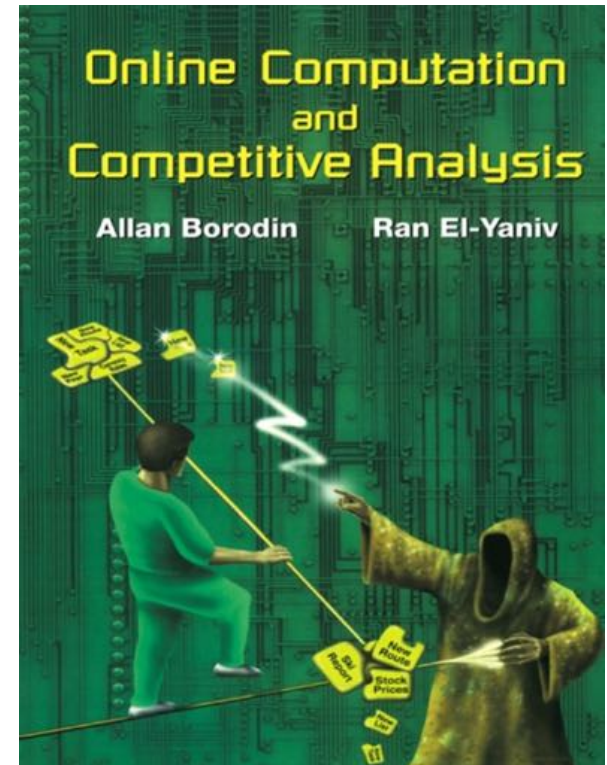
- approximation & online algorithms
- quality guaranties under uncertainty
- how to design & **analyze** optimization algorithms

Lecture

- definitions + theorems + proofs
- (black-/white-) board (+ slides)
- integrated exercises

Seminar

- block and/or running

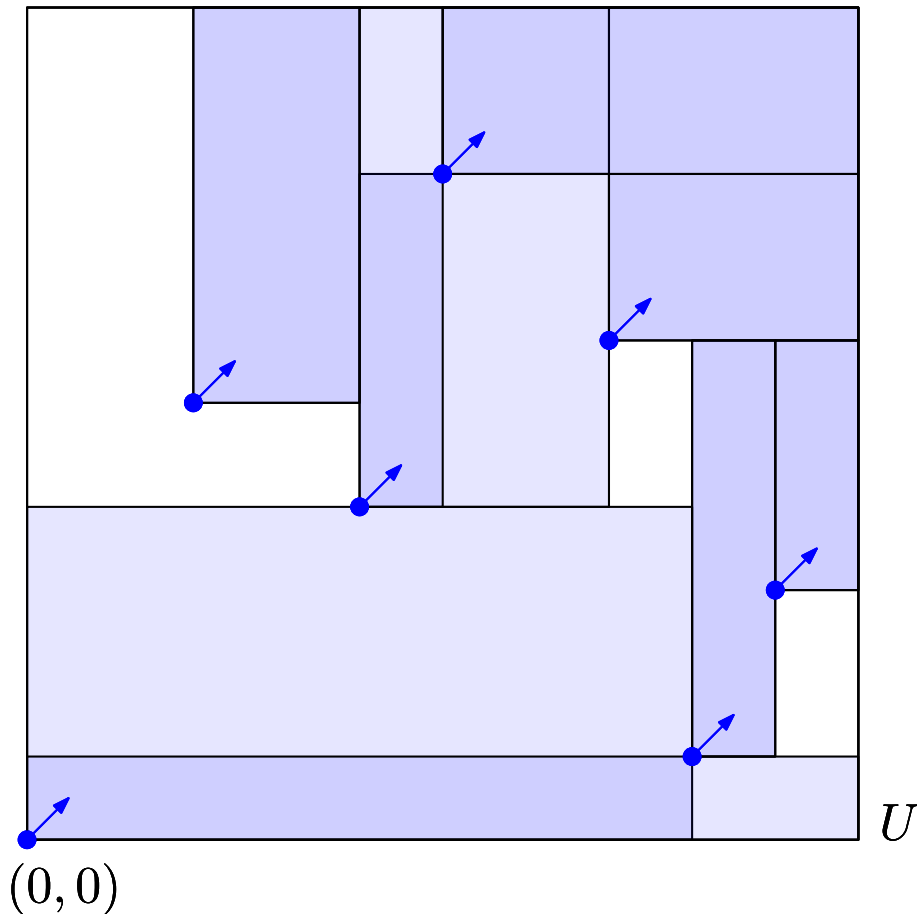


Research Examples

or: some Algorithmic Puzzles

Anchored Rectangle Packing

- n points in the unit square
- one of them at $(0,0)$



Objective

- for each point p , choose an axis-aligned rectangle with lower-left corner at p
- must be non-overlapping
- maximize covered area

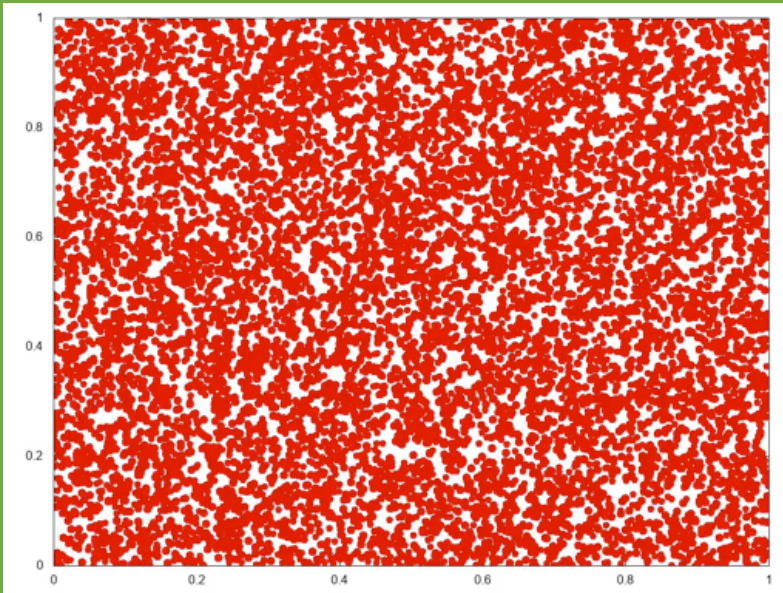
Randomized Gathering

- n robots in the plane
- act in discrete rounds
- instantaneous movement
- not necessarily local

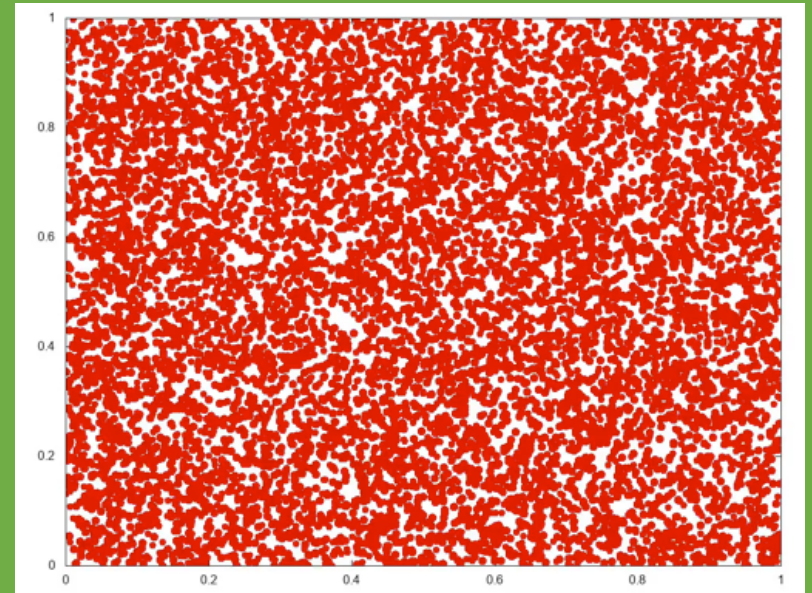
Objective:

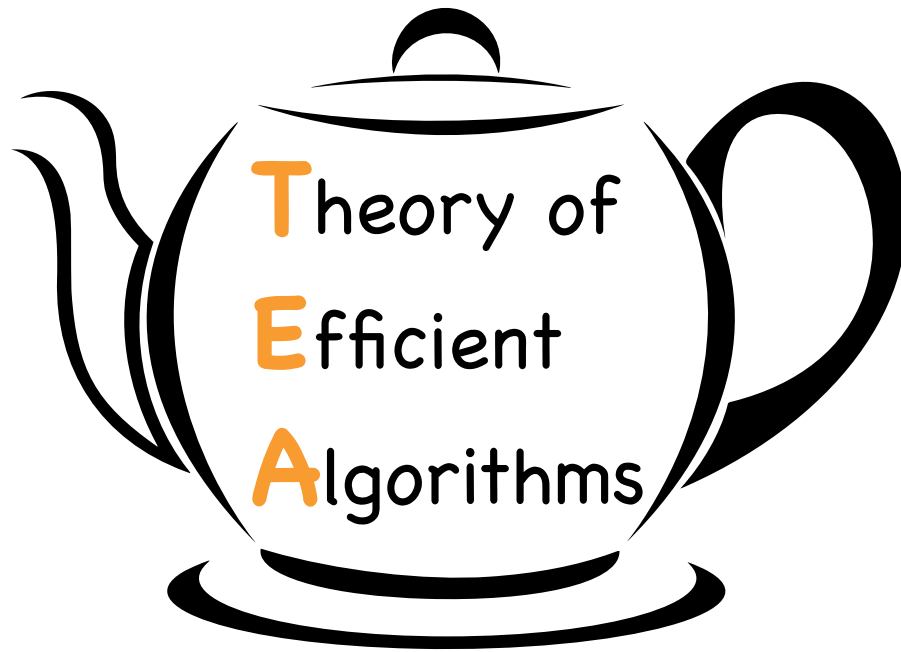
Gather in one point

Strategy 1:
go to random robot

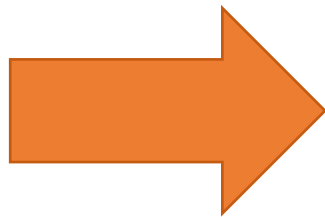


Strategy 2:
go to closest of two random robots





Questions



peter.kling@uni-hamburg.de