

Bereich Modelle und Algorithmen (MuA)

Vertreten durch 3 Fachgebiete

- Codes und Kryptographie (Blömer)**
- Algorithmen und Komplexität (Meyer auf der Heide)**
- Theorie verteilter Systeme (Scheideler)**

Zusätzlich eine Juniorprofessur

- Algorithmische Spieltheorie (Skopalik)**

Bereich Modelle und Algorithmen (MuA)



MuA Bachelormodul

**Datenstrukturen
und
Algorithmen**

**Einführung in Berechenbarkeit,
formale Sprachen und
Komplexität**

**Grundlegende
Algorithmen**

**Parallelität &
Kommunikation**

**Einführung in
Kryptographie**

**Methoden
des
Algorithmenentwurfs**

**Verteilte Algorithmen
und
Datenstrukturen**

Komplexitätstheorie

Optimierung

Ziel 2-3 Veranstaltungen pro Semester, 5-6 pro Jahr.

MuA ~~Master~~ ~~Produkt~~ ~~Teil~~

Datenstrukturen
und
Algorithmen

Einführung in Berechenbarkeit,
formale Sprachen und
Komplexität

Grundlegende
Algorithmen

Parallelität &
Kommunikation

Einführung in die
Kryptographie

Methoden
des
Algorithmen I
Algorithmen II

Verteilte Algorithmen
Algorithmen
in
Rechnernetzen

Komplexitätstheorie
Komplexität
und
Kryptographie

Ziel 2-3 Veranstaltungen pro Semester, 5-6 pro Jahr.

Angebot WS 2014/15 und Planung SS 2015

Vorlesungen WS 2014/15

- **Grundlegende Algorithmen (Meyer auf der Heide)**
- **Parallelität und Kommunikation (Meyer auf der Heide)**
- **Optimierung (Skopalik)**

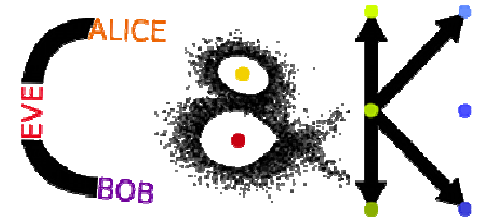
Proseminare WS 2014/15

- **Effiziente Algorithmen (Scheideler)**

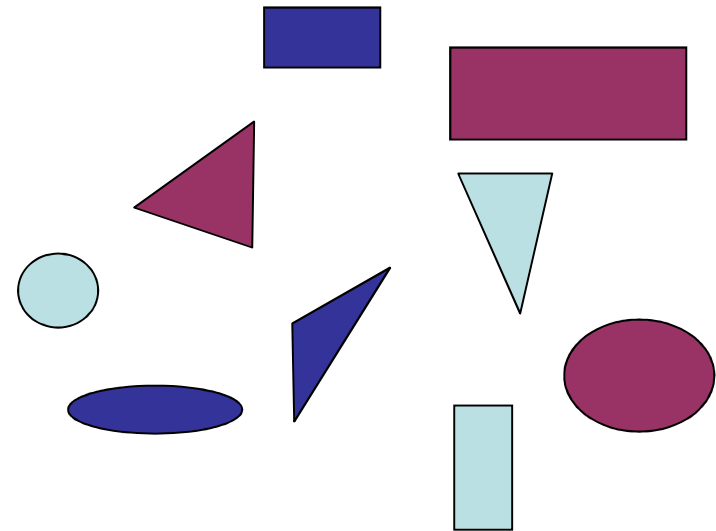


Vorlesungen SS 2015

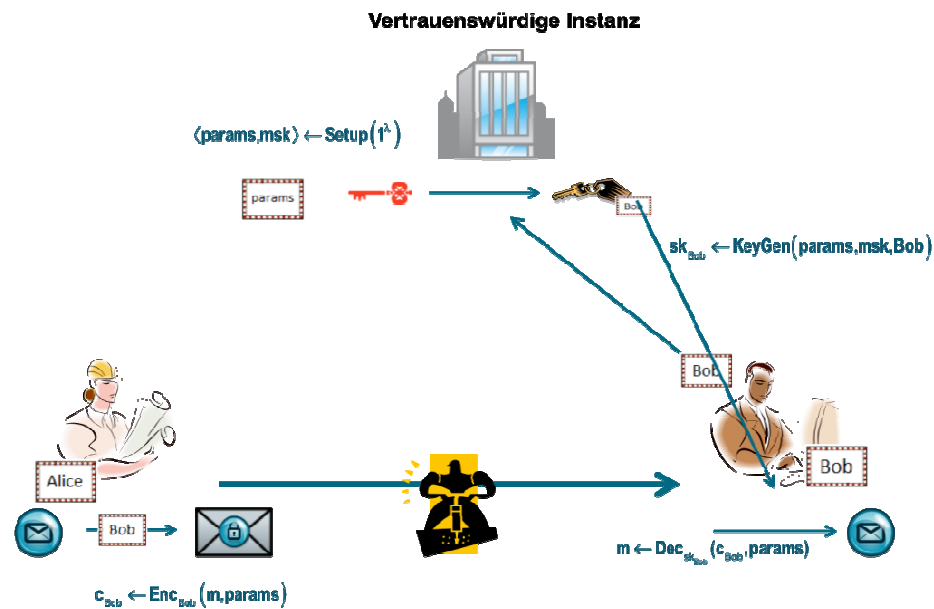
- **Methoden des Algorithmenentwurfs**
- **Einführung in Kryptographie**
- **Verteilte Algorithmen und Datenstrukturen**

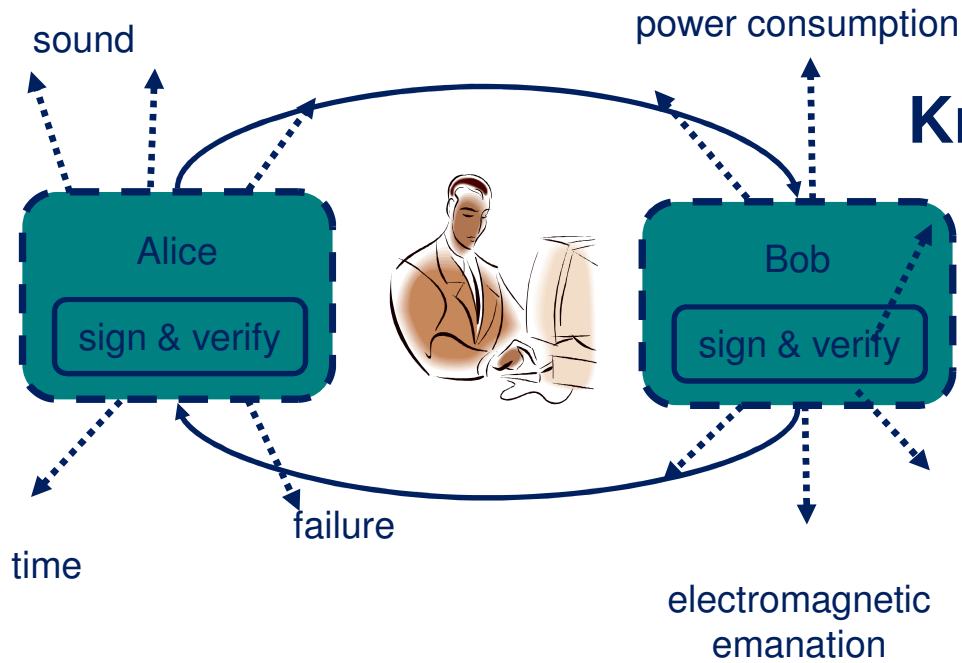
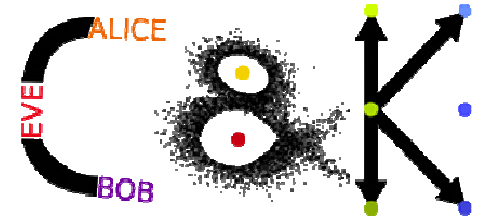


Clustering



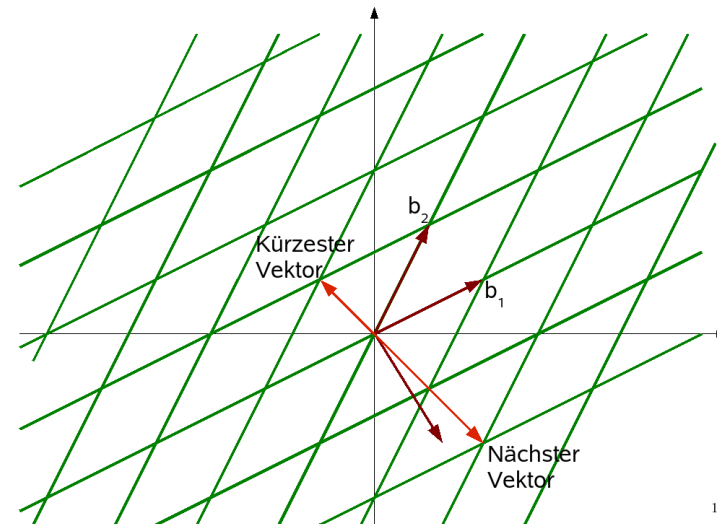
Identitätsbasierte Kryptographie





Kryptographie und Seitenkanäle

Kryptographie und Gitter



Hohe Rechenleistung
=
Innovative Computersysteme + Effiziente Algorithmen

Wir entwickeln und analysieren effiziente Algorithmen für innovative Computersysteme, evaluieren sie experimentell und stellen sie Anwendern zur Verfügung

- Innovative Computersysteme:
 - Dynamische Netzwerke wie mobile-ad-hoc Netze, vernetzte mobile Roboter, das Internet oder der Webgraph
 - Rechnernetze als Graphik-Hardware
- Methoden:
 - lokale verteilte Algorithmen
 - Randomisierung
 - Online und Approximationsalgorithmen



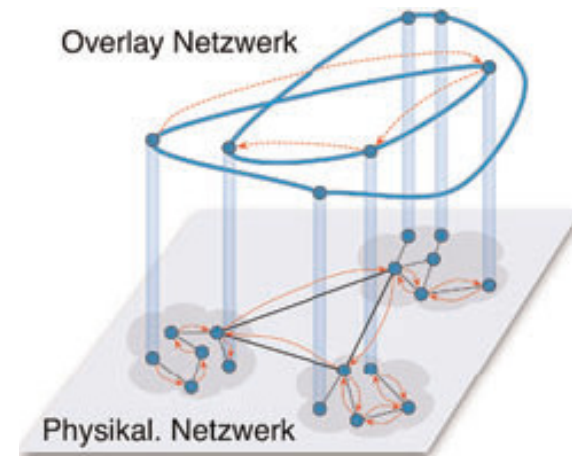
Dynamische und heterogene Netzwerke: Lokale Strategien für globale Aufgaben

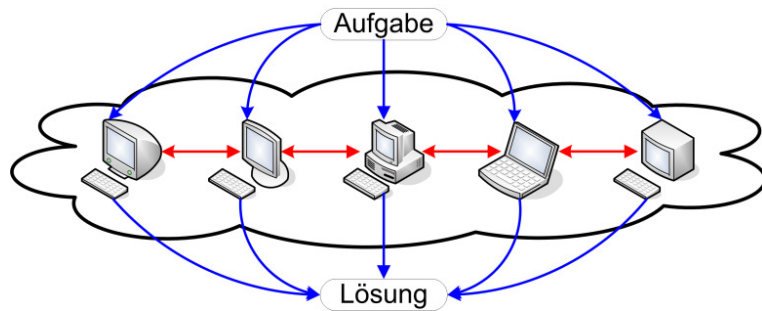
Problem: In einem großen dynamisch veränderlichen Netzwerk sollen globale Aufgaben gelöst werden. Allerdings ist keine globale Sicht auf das Netzwerk verfügbar.

Gesucht sind lokale Strategien, die zu global gutem Verhalten führen.

Beispiele:

- Mobile Roboter mit beschränkter Sichtweite sollen Zusammenhang aufrecht erhalten, sich auf verschiedene Aufgaben aufteilen (*Smart Teams*), sollen globale Daten für effizienten Zugriff dynamisch verteilen (*File Allocation*)
- Overlay Netze für Peer-to-Peer Systeme sollen ständig gute Kommunikationseigenschaften aufrecht erhalten (robuste Netze), wie z.B. Zusammenhang, hohe Expansion, gute Backbones und gute Spannbäume.

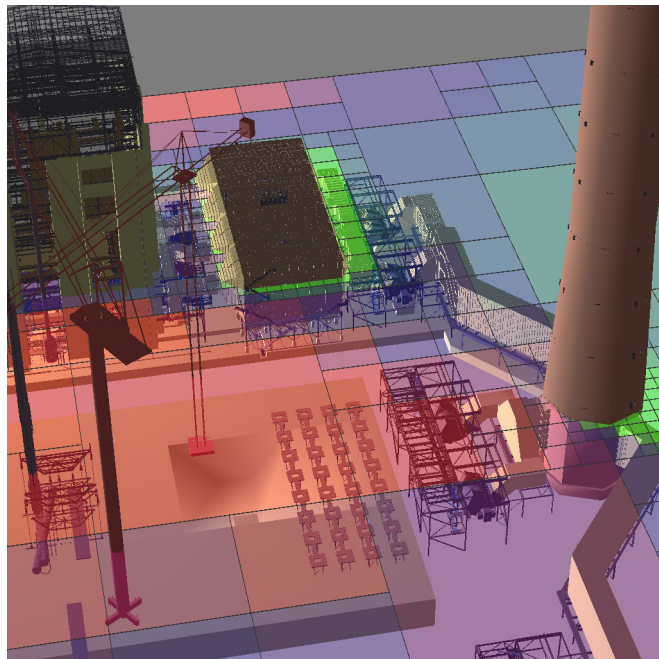




Peer-to-Peer basiertes paralleles Rechnen

Ungenutzte Rechenkapazität von Rechnern in großen Netzwerken soll für aufwendige Berechnungen genutzt werden.

Effiziente Ausführung erfordert lokale Lastbalancierung in dynamischen Netzen.

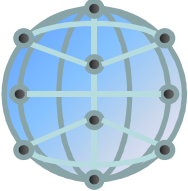


Algorithmen der Computergraphik

Problem: Die Effizienz der Darstellungsmethoden komplexer virtueller 3D-Welten hängt von der Charakteristik der Szene ab.

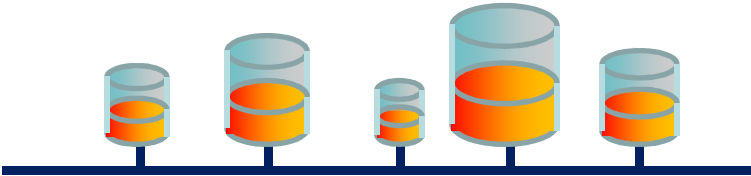
→ Gesucht sind Methoden, die die Charakteristik der Szene bestimmen und Renderingalgorithmen adaptiv auswählen.

Wir wenden unsere Methoden im Bereich der Simulation von Fertigungsanlagen und zur Darstellung von CAD-Modellen an.

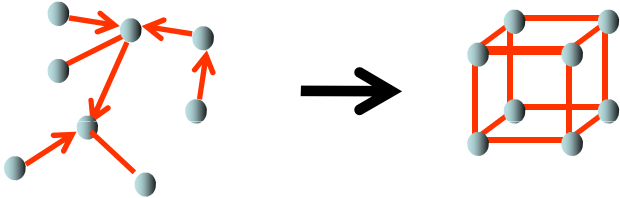


Forschungsprobleme

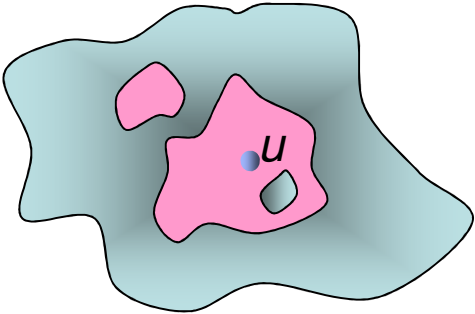
Verteilter Speicher



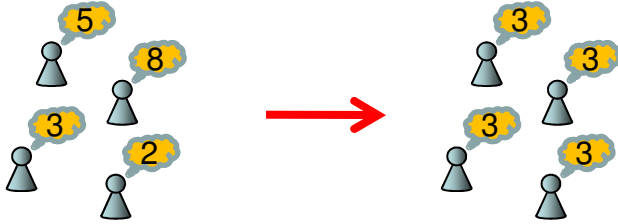
Selbstorganisierende Systeme

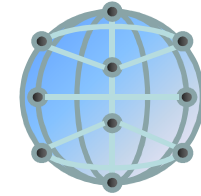


Funknetze



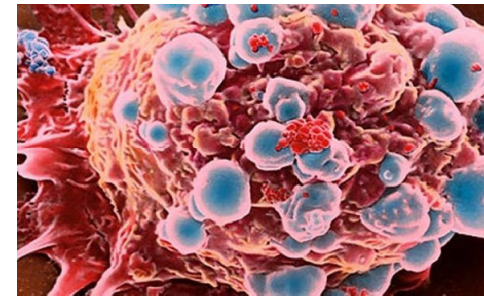
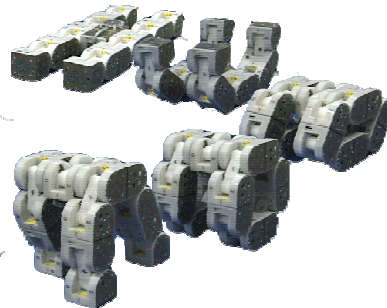
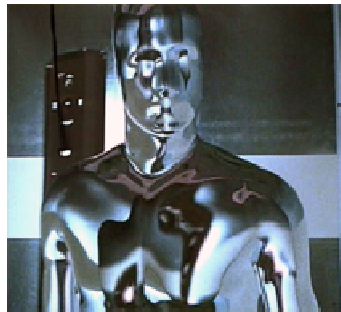
Verteilte Algorithmen
und Datenstrukturen





Forschungsprobleme

Selbstorganisierende Nanostrukturen



Modelle und Verfahren für robuste verteilte Systeme

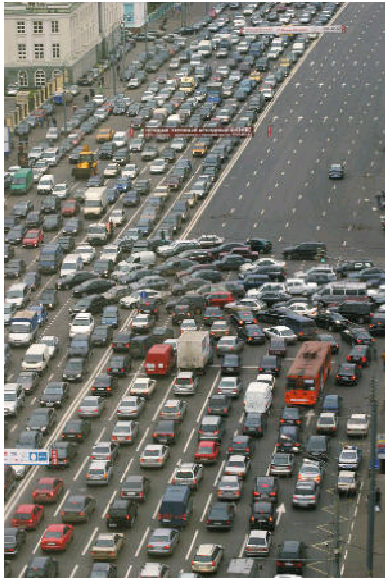
Systemstrategien:

- Redundanz
- Randomisierung
- Selbstheilung
- ...



Attacken:

- Denial-of-Service Attacken
- Identitätsüberschwemmung
- Protokollmanipulation
- ...



Algorithmische Spieltheorie

Problem:

- Das Ergebnis (z.B. eines Optimierungsproblems) wird bestimmt durch die Entscheidungen vieler einzelner Akteure.
- Diese wollen ihren eigenen Nutzen maximieren.
- Beispiel: Straßenverkehr.

Fragestellungen:

- Wie kann man das Ergebnis solcher verteilten Entscheidungen berechnen?
- Wie kann man gute Verfahren entwickeln, die berücksichtigen, dass Teilnehmer sich egoistisch verhalten?
- Wie schlecht sind die Ergebnisse solcher verteilten (egoistischen) Entscheidungen? Z.B. Im Vergleich mit einer zentral berechneten Lösung.