

# Verteilte Systeme – Übung

Tobias Distler, Klaus Stengel, Timo Hönig,  
Christopher Eibel, Tobias Klaus

Friedrich-Alexander-Universität Erlangen-Nürnberg  
Lehrstuhl Informatik 4 (Verteilte Systeme und Betriebssysteme)

[www4.cs.fau.de](http://www4.cs.fau.de)

Sommersemester 2013



## Wissenschaftliche Publikationen

- Was ist eine Publikation?

- Motivation für Publikationen

- Publikationsformen

## Wissenschaftliche Konferenzen

- Aufruf zur Einreichung von Arbeiten

- Kreuzgutachten und Begutachtungsprozess

- Organisation und Ablauf

## Lesen und Begutachten von Fachliteratur

- Lesen und Verstehen

- Verfassen eines Gutachtens

## Papierdiskussion



- Was ist eine wissenschaftliche Publikation?
  - schriftliche Arbeit
  - ein oder mehrere Autoren
  - Veröffentlichung
  - Vortrag
- Anspruch und Kriterien
  - Veröffentlichung neuer Erkenntnisse aus einem Forschungsgebiet
  - Qualitätssicherung (Stichwort: Kreuzgutachten)
  - Arbeit ist nachvollzieh- und belegbar, Quellen- bzw. Literaturverzeichnis
  - keine handwerklichen Fehler (Rechtschreibung, äußere Form)
- Gesellschaften und Verbände (relevant für Informatik)
  - ACM (Association for Computing Machinery)
  - IEEE (Institute of Electrical and Electronics Engineers)
  - GI (Gesellschaft für Informatik)



- Motivation für Publikationen
  - Präsentation von Forschungsergebnissen
  - Initiierung wissenschaftlicher Diskussionen
  - Einholen externer Meinungen
  - Zitierfähigkeit
  - Grundlage für Antragstellung (→ Forschungsgelder, „publish or perish“)
  
- Publikationsformen
  - Poster
  - Workshop- und Konferenzbeiträge, (→ Tagungsband, „Proceedings“)
  - Journal
  - Artikel in Fachzeitschrift
  - Buch



## Wissenschaftliche Publikationen

Was ist eine Publikation?

Motivation für Publikationen

Publikationsformen

## Wissenschaftliche Konferenzen

Aufruf zur Einreichung von Arbeiten

Kreuzgutachten und Begutachtungsprozess

Organisation und Ablauf

## Lesen und Begutachten von Fachliteratur

Lesen und Verstehen

Verfassen eines Gutachtens

## Papierdiskussion



- Aufruf zur Einreichung von Arbeiten (*Call for Papers*, kurz: *CFP*)
  - Eingrenzung der relevanten Interessengebiete
    - Zu welchen Forschungsbereichen sind Einreichungen gewünscht?
    - Welche Art von Arbeiten sind gefragt?
  - Details zum Ablauf der Begutachtung eingereicherter Arbeiten
  - Zusammensetzung von Programm- und Organisationskomitee
  - Abgabefristen, Abgaberrichtlinien (Anforderungen an Umfang und Format)
- Weitere optionale Inhalte
  - *Call for Workshops* (Aufruf zur Einreichung von Vorschlägen)
  - *Call for Posters* (Posterpräsentationen)
  - Stipendien



# Aufruf zur Einreichung von Arbeiten

- Aufruf zur Einreichung von Arbeiten (*Call for Papers*, kurz: *CFP*)
  - Eingrenzung der relevanten Interessengebiete
    - Zu welchen Forschungsbereichen sind Einreichungen gewünscht?
    - Welche Art von Arbeiten sind gefragt?
  - Details zum Ablauf der Begutachtung eingereicherter Arbeiten
  - Zusammensetzung von Programm- und Organisationskomitee
  - Abgabefristen, Abgaberrichtlinien (Anforderungen an Umfang und Format)
- Weitere optionale Inhalte
  - *Call for Workshops* (Aufruf zur Einreichung von Vorschlägen)
  - *Call for Posters* (Posterpräsentationen)
  - Stipendien
- Beispiel: European Conference on Computer Systems (EuroSys'12)
  - Webseite:  
<http://eurosys2012.unibe.ch/>
  - Call for Papers:  
<http://eurosys2012.unibe.ch/calls/papers>



- Kreuzgutachten (*Peer-Review*)
  - Begutachtung der eingereichten Arbeiten (Mehr-Augen-Prinzip)
  - Feststellung der Qualität **und** Eignung eingereicherter Forschungsarbeiten
  - Begutachtungsmodus
    - Blindgutachten (*Single-Blind*)
    - Doppeltblindgutachten (*Double-Blind*)
  - Befangenheit vermeiden
    - Gewährleistung von Objektivität und Fairness
    - Eingereichte Arbeit stammt von einem Forscher, der den Gutachter kennt
- Begutachtungsprozess
  - Eine oder mehrere Begutachtungsrunden
  - Regeln für den Ausschluss eingereicherter Arbeiten (Ablehnung)
  - Benachrichtigung der Autoren (*Notification*)
  - Bekanntmachung der angenommenen Arbeiten
- Publikation
  - Veröffentlichung besteht aus schriftlicher Arbeit **und** Vortrag
  - Akzeptierte Arbeiten erscheinen in einem Tagungsband (*Proceedings*)





- *Double-Blind-Modus*
  - Autoren wissen nicht, wer die Reviews geschrieben hat
  - Reviewer wissen nicht, von wem die Papiere stammen
- Reviewer
  - 37 Programmkomitee-Mitglieder
  - 83 externe Reviewer
- Stufenweiser Prozess
  - Runde 1: Aussortieren der „schlechten“ Papiere (drei Reviews pro Papier)
  - Runde 2: Einholen weiterer Meinungen (zwei Reviews pro Papier)
  - Runde 3: Zusätzliche Reviews zu umstrittenen Papieren
  - Rebuttal: Erwiderung der Autoren auf die Reviews
  - Programmkomitee-Treffen: Besprechung der Reviews, endgültige Auswahl
- Statistik
  - 179 eingereichte Beiträge
  - 96 Papiere erreichten die 2. Runde
  - 27 Papiere wurden am Ende akzeptiert (ca. 15 % der Einreichungen)
  - Mehr als 750 Reviews



- Vortragsmodus
  - Single-Track: Zu einem Zeitpunkt nur ein Vortrag
  - Multi-Track: Parallel stattfindende *Sessions*



# Organisation und Ablauf der Konferenz

- Vortragsmodus
  - Single-Track: Zu einem Zeitpunkt nur ein Vortrag
  - Multi-Track: Parallel stattfindende *Sessions*

WEDNESDAY, APRIL 11, 2012

08:00 - 08:30

REGISTRATION

08:30 - 09:00

OPENING

09:00 - 10:00

SESSION 1: TRANSACTIONS (CHAIR: ANNE-MARIE KERMARREC)

- [STM in the small: trading generality for performance in software transactional memory](#)  
*Aleksandar Dragojevic (EPFL) and Tim Harris (Microsoft Research)*
- [Improving Server Applications with System Transactions](#)  
*Sangman Kim, Michael Lee, Alan Dunn, and Owen S. Hofmann (The University of Texas at Austin),  
Xuan Wang (Stony Brook University), Emmett Witchel (The University of Texas at Austin), and  
Donald E. Porter (Stony Brook University)*

10:00 - 10:30

COFFEE

10:30 - 12:00

SESSION 2: EVERYTHING GREEN: ENERGY MATTERS (CHAIR: HERMANN HÄRTIG)

- [Where is the energy spent inside my app? Fine Grained Energy Accounting on Smartphones with Eprof](#)  
*Abhinav Pathak and Y. Charlie Hu (Purdue University) and Ming Zhang (Microsoft Research)*
- [Energy Efficiency for Large-Scale MapReduce Workloads with Significant Interactive Analysis](#)  
*Yanpei Chen and Sara Alspaugh (UC Berkeley), Dhruba Borthakur (Facebook), and Randy Katz (UC Berkeley)*
- [GreenHadoop: Leveraging Green Energy in Data-Processing Frameworks](#)  
*Inigo Goiri, Kien Le, and Thu D. Nguyen (Rutgers University), Jordi Guitart and Jordi Torres (UPC),  
and Ricardo Bianchini (Rutgers University)*

12:00 - 13:30

LUNCH

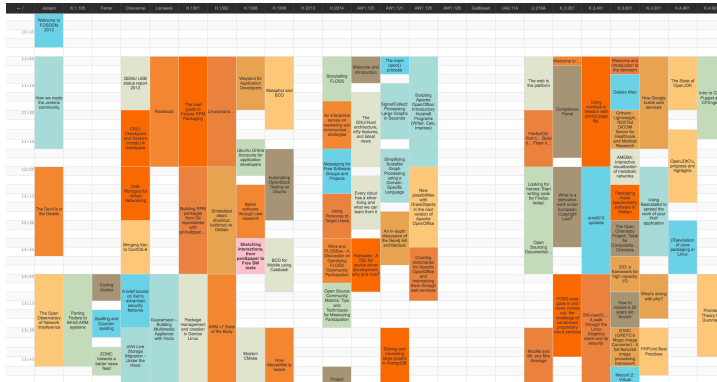
## EuroSys 2012: Single-Track-Programm eines Vormittages



# Organisation und Ablauf der Konferenz

## Vortragsmodus

- Single-Track: Zu einem Zeitpunkt nur ein Vortrag
- Multi-Track: Parallel stattfindende Sessions



FOSDEM 2012: Multi-Track-Programm eines Vormittages



- Vortragsmodus
  - Single-Track: Zu einem Zeitpunkt nur ein Vortrag
  - Multi-Track: Parallel stattfindende *Sessions*
  
- Vortragsprogramm
  - Workshops
    - Single-Track
    - **Multi-Track**
  - Konferenz
    - **Single-Track**
    - Multi-Track
  
- Rahmenprogramm
  - *Social Event* (z. B. gemeinsames Abendessen, kulturelles Programm)
  - Mitgliederversammlung
  - Auszeichnungen der besten Arbeiten (z. B. *Best Paper Award*)



## Wissenschaftliche Publikationen

Was ist eine Publikation?

Motivation für Publikationen

Publikationsformen

## Wissenschaftliche Konferenzen

Aufruf zur Einreichung von Arbeiten

Kreuzgutachten und Begutachtungsprozess

Organisation und Ablauf


## Lesen und Begutachten von Fachliteratur

Lesen und Verstehen

Verfassen eines Gutachtens

## Papierdiskussion



- Gründe ein Papier zu lesen
  - Literaturanalyse relevanter verwandter Arbeiten
  - Begutachtung von zur Veröffentlichung eingereichten Beiträgen
  - [Weil es für die Verteilte-Systeme-Übung notwendig ist.]
  - ...
- Mögliche Herangehensweise: Mindestens drei Lesedurchgänge mit jeweils unterschiedlichem Fokus
  - 1. Durchgang: Erster allgemeiner Eindruck
  - 2. Durchgang: Überblick über den Inhalt
  - 3. Durchgang: Detailliertes Verständnis
- Literatur
  -  Srinivasan Keshav  
**How to Read a Paper**  
*ACM SIGCOMM Computer Communication Review*, 37(3):83–84, 2007.



# 1. Lesedurchgang

---

- Ziel: Verschaffen eines ersten allgemeinen Eindrucks
- Interessante Fragestellungen
  - In welche Kategorie (z. B. Analyse eines bereits existierenden Systems, Beschreibung eines Prototyps, etc.) fällt das Papier?
  - Was ist der wissenschaftliche Beitrag des Papiers?
  - Sind die getroffenen Annahmen dem ersten Anschein nach berechtigt?
  - Mit welchen anderen Papieren ist das Papier thematisch verwandt?
- Vorgehensweise
  - Detailliertes Lesen
    - Titel
    - Abstract
    - Einleitung
    - Schluss
  - Kurzer Blick auf
    - Überschriften
    - Referenzen





## 2. Lesedurchgang

---

- Ziel: Verschaffen eines Überblicks über den Inhalt
- Interessante Fragestellungen
  - Was ist der (komplette) Inhalt des Papiers?
  - Wie würde ich einem anderen den Inhalt des Papiers erklären?
  - Enthält das Papier offensichtliche Fehler?
- Vorgehensweise
  - Detailliertes Lesen bzw. Betrachten
    - Abschnitte aus 1. Lesedurchgang
    - Restliche Abschnitte
    - Abbildungen, Graphen, etc.
  - Aussparen von Details (z. B. Beweisen)
  - Notizen
    - Zentrale Punkte
    - Relevante Referenzen
    - Unklare Stellen



### 3. Lesedurchgang

---

- Ziel: Detailliertes Verständnis des Papiers
- Interessante Fragestellungen
  - Ist das Papier in sich stimmig aufgebaut?
  - Sind die auf Basis der Annahmen gezogenen Schlüsse korrekt?
  - Werden Annahmen getroffen, die nicht explizit erwähnt sind?
  - Sind alle Nachteile des präsentierten Ansatzes ausreichend diskutiert?
  - Wie hätte ich den wissenschaftlichen Beitrag des Papiers präsentiert?
- Vorgehensweise
  - Besonderes Augenmerk auf Details
  - Hinterfragen sämtlicher Behauptungen
  - (Gedankliches) Nachvollziehen der präsentierten Experimente
  - Heranziehen von referenzierten verwandten Arbeiten



### 3. Lesedurchgang

---

- Ziel: Detailliertes Verständnis des Papiers
- Interessante Fragestellungen
  - Ist das Papier in sich stimmig aufgebaut?
  - Sind die auf Basis der Annahmen gezogenen Schlüsse korrekt?
  - Werden Annahmen getroffen, die nicht explizit erwähnt sind?
  - Sind alle Nachteile des präsentierten Ansatzes ausreichend diskutiert?
  - Wie hätte ich den wissenschaftlichen Beitrag des Papiers präsentiert?
- Vorgehensweise
  - Besonderes Augenmerk auf Details
  - Hinterfragen sämtlicher Behauptungen
  - (Gedankliches) Nachvollziehen der präsentierten Experimente
  - Heranziehen von referenzierten verwandten Arbeiten
- **Abhängig vom eigenen Vorwissen und der Qualität des Papiers müssen eventuell weitere Lesedurchgänge folgen...**



- Einsatz von Gutachten (*Reviews*)
  - Begründung für die Akzeptanz bzw. Ablehnung eines zur Veröffentlichung eingereichten wissenschaftlichen Papiers
  - Präsentation von Verbesserungsvorschlägen
- Ansprüche an ein Review
  - Nachvollziehbarkeit
  - Fairness
  - Sachlichkeit
  - ...

## ■ Literatur



Timothy Roscoe

**Writing Reviews for Systems Conferences**

<http://people.inf.ethz.ch/troscoe/pubs/review-writing.pdf>, 2007.



# Aufbau eines Review

## ■ Gesamturteil und Vorkenntnisse

Strong accept
Accept
Weak accept
Weak reject
Reject
Strong reject

Expert
Knowledgable
Some Familiarity
No Familiarity

## ■ Kurze Zusammenfassung des Papiers

- Nachweis, dass der Reviewer das Papier (gelesen und) verstanden hat
- Objektive Beschreibung des Inhalts
- Nennung des (von den Autoren angeführten) wissenschaftlichen Beitrags

## ■ Überblick über Stärken und Schwächen

## ■ Detaillierte Kommentare

## ■ Handwerkliche Fehler

- Rechtschreib- und Grammatikfehler
- Zu kleine Abbildungen
- ...



- Vorbereitung
  - Papier (mehrfach) lesen
  - Notizen machen
    - Unklare Stellen markieren
    - Offene Fragen festhalten [Auch wenn sie vielleicht weiter hinten im Papier geklärt werden.]
    - Fehler anstreichen
  - Verwandte Arbeiten lesen bzw. suchen
- Review verfassen
  - Aussagen begründen
  - Positive statt negative Formulierungen verwenden
  - Fragen stellen statt Befehle geben
  - Nach Möglichkeit Verbesserungsvorschläge machen  
[Es ist jedoch nicht notwendig die Arbeit der Autoren zu machen.]
  - Positives hervorheben
  - Nichtssagende Formulierungen vermeiden

“The evaluation could really be beefed up.”



## ■ Inhalt

- Neuer wissenschaftlicher Beitrag (*Novelty*)
  - Lösung eines relevanten, bisher ungelösten Problems
  - Neue (bessere) Lösung eines relevanten, bereits gelösten Problems
- Geeignete Lösung für das adressierte Problem
  - Valide, möglichst schwache Annahmen
  - Lösungsansatz enthält keine technischen Fehler
  - Evaluationsergebnisse belegen die Vor- und Nachteile der Lösung
- Ausreichende Diskussion verwandter Arbeiten

## ■ Stil

- Überzeugende Motivation des adressierten Problems
- Ausreichende Einführung in den Themenkomplex
- Explizite Erläuterung der gemachten Annahmen
- Klare Präsentation der Lösung
- Nachvollziehbare Beschreibung der Evaluation



# Der feindlich gesinnte Reviewer

---

- Auszüge aus



Graham Cormode

**How NOT to Review a Paper:**

**The Tools and Techniques of the Adversarial Reviewer**

*SIGMOD Record*, 37(4):100–104, 2008.

- Blind Reviewing





- Auszüge aus



Graham Cormode

**How NOT to Review a Paper:**

**The Tools and Techniques of the Adversarial Reviewer**

*SIGMOD Record*, 37(4):100–104, 2008.

- Blind Reviewing

“The skilled adversarial reviewer can find reasons to reject any paper **without even reading it**. This is considered **truly blind reviewing**. [...]”



- Auszüge aus



Graham Cormode

**How NOT to Review a Paper:**

**The Tools and Techniques of the Adversarial Reviewer**

*SIGMOD Record*, 37(4):100–104, 2008.

- Blind Reviewing

“The skilled adversarial reviewer can find reasons to reject any paper **without even reading it**. This is considered **truly blind reviewing**. [...]”

“[...] ‘This paper **leaves many questions unanswered**.’ In particular, **the questions that have not been asked**. [...]”



# Der feindlich gesinnte Reviewer

## ■ Auszüge aus



Graham Cormode

**How NOT to Review a Paper:**

**The Tools and Techniques of the Adversarial Reviewer**

*SIGMOD Record*, 37(4):100–104, 2008.

## ■ Blind Reviewing

“The skilled adversarial reviewer can find reasons to reject any paper **without even reading it**. This is considered **truly blind reviewing**. [...]”

“[...] ‘This paper **leaves many questions unanswered**.’ In particular, **the questions that have not been asked**. [...]”

“[...] ‘The paper is of **limited interest**.’ Since, at most, **only Computer Scientists** are likely to be interested in the paper. [...]”



# Der feindlich gesinnte Reviewer

## ■ Auszüge aus



Graham Cormode

**How NOT to Review a Paper:**

**The Tools and Techniques of the Adversarial Reviewer**

*SIGMOD Record*, 37(4):100–104, 2008.

## ■ Blind Reviewing

“The skilled adversarial reviewer can find reasons to reject any paper **without even reading it**. This is considered **truly blind reviewing**. [...]”

“[...] ‘This paper **leaves many questions unanswered**.’ In particular, **the questions that have not been asked**. [...]”

“[...] ‘The paper is of **limited interest**.’ Since, at most, **only Computer Scientists** are likely to be interested in the paper. [...]”

## ■ Vorkenntnisse

“[...] The adversarial reviewer always marks themselves as an **‘expert’ on every topic**, even ones which they have never heard of before. [...]”



- Verwandte Arbeiten



- Verwandte Arbeiten

“[...] [Reviewers] can suggest some **papers with absolutely no relation** to the submission, and leave the authors scratching their heads. [...]”



## ■ Verwandte Arbeiten

“[...] [Reviewers] can suggest some **papers with absolutely no relation** to the submission, and leave the authors scratching their heads. [...]”

## ■ Nie zufrieden sein!

“[...] **Examples.** If there are few or no examples, the reviewer complains ‘There are **insufficient examples to illustrate what is meant**’; but if there are many, then the complaint is ‘There are too many **obvious examples which interrupt the flow of the paper**’. [...]”



## ■ Verwandte Arbeiten

“[...] [Reviewers] can suggest some **papers with absolutely no relation** to the submission, and leave the authors scratching their heads. [...]”

## ■ Nie zufrieden sein!

“[...] **Examples.** If there are few or no examples, the reviewer complains ‘There are **insufficient examples to illustrate what is meant**’; but if there are many, then the complaint is ‘There are too many **obvious examples which interrupt the flow of the paper**’. [...]”

“[...] **Experiments.** Either ‘Only a **few experiments which do not convince that this method works** over a broad variety of data’ or else ‘**Too many plots which show the same results** over and over again for minor variations of the setup do not give useful information.’ [...]”





# Der feindlich gesinnte Reviewer

## ■ Verwandte Arbeiten

“[...] [Reviewers] can suggest some **papers with absolutely no relation** to the submission, and leave the authors scratching their heads. [...]”

## ■ Nie zufrieden sein!

“[...] **Examples.** If there are few or no examples, the reviewer complains ‘There are **insufficient examples to illustrate what is meant**’; but if there are many, then the complaint is ‘There are too many **obvious examples which interrupt the flow of the paper**’. [...]”

“[...] **Experiments.** Either ‘Only a **few experiments which do not convince that this method works** over a broad variety of data’ or else ‘**Too many plots which show the same results** over and over again for minor variations of the setup do not give useful information.’ [...]”

“[...] The adversarial reviewer [...] complains that the **plots were too small to read**, and so it was impossible to draw any conclusions about the experiments. For added measure, the reviewer will affect to **suffer from color-blindness**, and so cannot tell which line is which. [...]”



# Als Reviewer kann man sich irren...

---

- Auszüge aus



Simone Santini

**We Are Sorry to Inform You...**

*Computer*, 38(12):126-128, 2005.

- Edsger W. Dijkstra, *Goto Statement Considered Harmful*.



- Auszüge aus



Simone Santini

**We Are Sorry to Inform You...**

*Computer*, 38(12):126-128, 2005.

- Edsger W. Dijkstra, *Goto Statement Considered Harmful*.

“This paper tries to convince us that **the well-known goto statement** should be eliminated from our programming languages or, at least (since **I don't think that it will ever be eliminated**), that programmers should not use it. [...]”



- Auszüge aus



Simone Santini

**We Are Sorry to Inform You...**

*Computer*, 38(12):126-128, 2005.

- Edsger W. Dijkstra, *Goto Statement Considered Harmful*.

“This paper tries to convince us that **the well-known goto statement** should be eliminated from our programming languages or, at least (since **I don't think that it will ever be eliminated**), that programmers should not use it. [...]”

“[...] More than 10 years of **industrial experience with Fortran** have proved conclusively to everybody concerned that, in the real world, **the goto is useful and necessary** [...]”



- Auszüge aus



Simone Santini

**We Are Sorry to Inform You...**

*Computer*, 38(12):126-128, 2005.

- Edsger W. Dijkstra, *Goto Statement Considered Harmful*.

“This paper tries to convince us that **the well-known goto statement** should be eliminated from our programming languages or, at least (since **I don't think that it will ever be eliminated**), that programmers should not use it. [...]”

“[...] More than 10 years of **industrial experience with Fortran** have proved conclusively to everybody concerned that, in the real world, **the goto is useful and necessary** [...]”

“[...] Publishing this would waste valuable paper: Should it be published, **I am as sure it will go uncited and unnoticed** as I am confident that, 30 years from now, the goto will still be alive and well and used as widely as it is today. [...]”



## Als Reviewer kann man sich irren...

---

- Ronald L. Rivest, Adi Shamir, and Leonard Adelman  
*A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.*



## Als Reviewer kann man sich irren...

- Ronald L. Rivest, Adi Shamir, and Leonard Adelman  
*A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.*

“According to the (very short) introduction, this paper purports to present a ***practical implementation*** of Diffie and Hellman’s public-key cryptosystem for applications in the electronic mail realm. [...] **I doubt that a system such as this one will ever be *practical*.** [...]”



# Als Reviewer kann man sich irren...

- Ronald L. Rivest, Adi Shamir, and Leonard Adelman

*A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.*

“According to the (very short) introduction, this paper purports to present a **practical implementation** of Diffie and Hellman’s public-key cryptosystem for applications in the electronic mail realm. [...] **I doubt that a system such as this one will ever be practical.** [...]”

“[...] Finally, there is the question of the application. Electronic mail on the Arpanet is indeed a **nice gizmo, but it is unlikely it will ever be diffused outside academic circles** and public laboratories [...] Granted, we are seeing the appearance of so-called *microcomputers*, such as the recently announced Apple II, but their limitations are so great that neither they nor their descendants **will have the power necessary to communicate through a network.** [...]”





# Als Reviewer kann man sich irren...

- Ronald L. Rivest, Adi Shamir, and Leonard Adelman

*A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.*

“According to the (very short) introduction, this paper purports to present a *practical implementation* of Diffie and Hellman’s public-key cryptosystem for applications in the electronic mail realm. [...] **I doubt that a system such as this one will ever be practical.** [...]”

“[...] Finally, there is the question of the application. Electronic mail on the Arpanet is confused outside seeing the ap ed Ap- ple II, ndants will h k. [...]”

The screenshot shows a Google Scholar search interface. At the top, there are tabs for 'Web', 'Images', and 'More...'. The Google logo is on the left, followed by a search bar and a search button. Below the search bar, it says 'Scholar' and 'About 256 results (0.24 sec)'. Underneath, there are two search results. The first result is titled 'A method for obtaining digital signatures and public-key cryptosystems' by 'RL Rivest, A Shamir, L Adleman - Communications of the ACM, 1978 - dl.acm.org'. It includes an abstract: 'Abstract An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:(1) Couriers or other secure means are not needed to transmit ...'. Below the abstract are links for 'Cited by', 'Related articles', 'Import into BibTeX', and 'More'. The second result is a PDF version of the same paper, titled 'PDF A Method for Obtaining Digital Signatures and Public-Key Cryptosystems' by 'RL Rivest, A Shamir, L Adleman - Communications, 1978 - cs.usu.edu.ru'. It includes a similar abstract: 'An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:(1) Couriers or other secure means are not needed to transmit ...'.



# Als Reviewer kann man sich irren...

- Ronald L. Rivest, Adi Shamir, and Leonard Adelman

*A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.*

“According to the (very short) introduction, this paper purports to present a *practical implementation* of Diffie and Hellman’s public-key cryptosystem for applications in the electronic mail realm. [...] **I doubt that a system such as this one will ever be practical.** [...]”

“[...] Finally, there is the question of the application. Electronic mail on the ARPANET is not a secure communication channel. [...] I have discussed seeing [...] ed Ap- [...] ndants [...] k. [...]”

The screenshot shows a Google Scholar search result. At the top, there are tabs for 'Web', 'Images', and 'More...'. Below them is the Google logo and a search bar with a magnifying glass icon. The search results are displayed under the 'Scholar' heading, indicating 'About 256 results (0.24 sec)'. Under 'All versions', two entries are shown. The first entry is titled 'A method for obtaining digital signatures and public-key cryptosystems' by 'RL Rivest, A Shamir, L Adleman - Communications of the ACM, 1978 - dl.acm.org'. It includes an abstract snippet: 'Abstract An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:(1) Couriers or other secure means are not needed to transmit ...'. Below the abstract, it says 'Cited by 12198' (with '12198' in a red box), 'Related articles', 'Import into BibTeX', and 'More ▾'. The second entry is a PDF version of the same paper, titled 'A Method for Obtaining Digital Signatures and Public-Key Cryptosystems' by 'RL Rivest, A Shamir, L Adleman - Communications, 1978 - cs.usu.edu.ru'. It also includes the same abstract snippet.



# Vorbereitung der Papierdiskussion

- Papier (→ /proj/i4vs/pub) lesen und verstehen
  - 📄 Tongping Liu, Charlie Curtsinger, and Emery D. Berger  
**Dthreads: Efficient Deterministic Multithreading**  
*Proceedings of the 23rd Symposium on Operating Systems Principles, 2011.*
  - Deterministische Ausführung mehrfädiger C/C++-Programme
  - Alternative zur pthreads-Bibliothek
- Aufgabenstellung: Verfassen eines Review
  - Aufbau
    - Gesamturteil:  $\{Strong, , Weak\} Reject, \{Weak, , Strong\} Accept$
    - Kurze Zusammenfassung des Inhalts (höchstens 5 Sätze)
    - Kurzbegründung des Urteils: Liste der Stärken und Schwächen (Stichpunkte)
    - Detaillierte Kommentare zum Papier
  - Anforderungen
    - Ein Review (deutsch *oder* englisch) pro Übungsgruppe
    - Gesamtumfang: mindestens 600 Wörter
- Ablauf
  - Abgabe des Review: bis **spätestens 17.06.** bzw. **19.06.**
  - Abgabe per E-Mail: `vs@i4.informatik.uni-erlangen.de`
  - Papierdiskussion: am 18.06. bzw. 20.06. in der Tafelübung

