

# Semantics and Verification

## The Dat 5/SSE 3 course

*How to read and present a scientific paper*

Hans Hüttel – based on original slides by Emmanuel Fleury

Department of Computer Science, Aalborg University

# **Part I:**

# **Read a Scientific Paper**

# Motivations

## Why Read Scientific Papers ?

[Academia]

I read papers because of:

- The Content:

To look for new **ideas** or new **proof techniques** to write a new paper

- The Topic:

To look for new **directions** within my field or to learn a new **topic**

- The Authors:

To look for **valuable colleagues** to work with or **newcomers**

# Motivations

## Why Read Scientific Papers ?

[Company World]

I read papers because of:

- The Content:

I need the most **efficient algorithm** or **new techniques** for my product

- The Topic:

Can I get a **new product** out of these research results? ?

- The Authors:

Who are the **valuable persons** to hire or collaborate with ?

# Motivations

Why bother ?

I already know how to read English !!!

**Scientific papers are cryptic ...**

(notation, maths, references to other papers, ...)

**... and not always easy to find ...**

(where to find good papers ?)

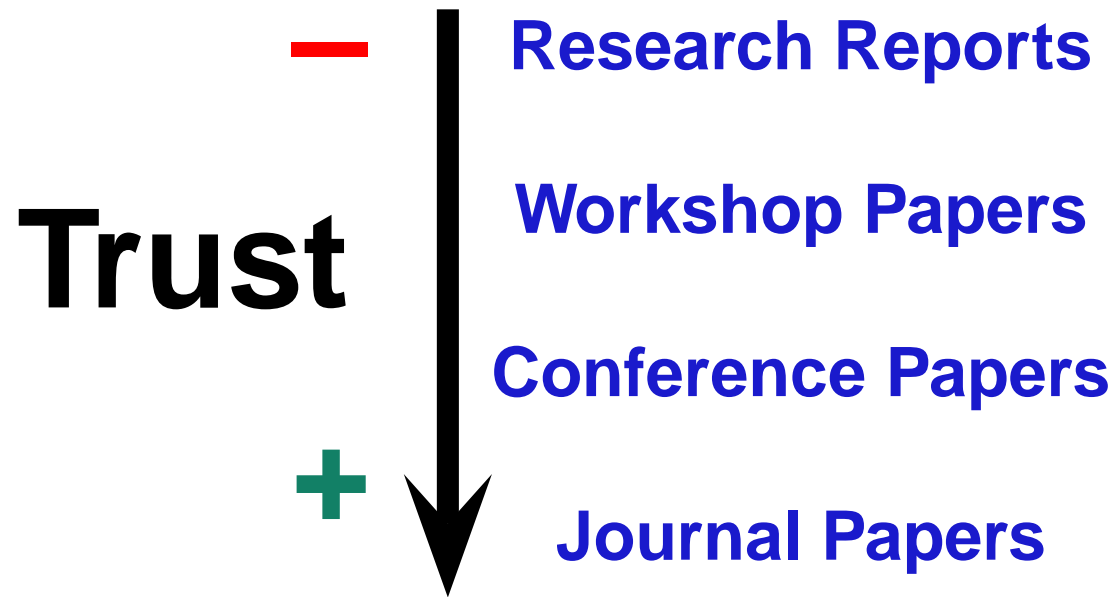
**... and complex.**

(theorems, lemmas, proofs, experiments, ...)

# Plan

1. Taxonomy of Scientific Papers
2. Structure of Scientific Papers
3. First Read Through
4. In-depth Reading
5. Looking at References
6. Evaluating Scientific Papers
7. Annexes
  - How to Read a Proof
  - How to Read an Experimental Result

# Taxonomy of Scientific Papers



# Taxonomy of Scientific Papers

## Research Reports

- Review:** None
- Goal:** Stamp an idea before publishing
- Size:** Depends
- Freshness:** Instantaneous

## Workshop Papers

- Review:** Yes, but often low threshold
- Goal:** Either submit “*in progress*” work and hoping for feedback, or the paper has been rejected for a conference (some workshops are actually small conferences)
- Size:** Few pages (from 5 to 15)
- Freshness:** From few weeks to few months



# Taxonomy of Scientific Papers

## Conference Papers

- Review:** Yes, but threshold depends on the conference  
(some are best avoided!)
- Goal:** Publish finished work with possible forthcoming research
- Size:** More than 8 pages and less than 20
- Freshness:** Few months

## Journal Papers

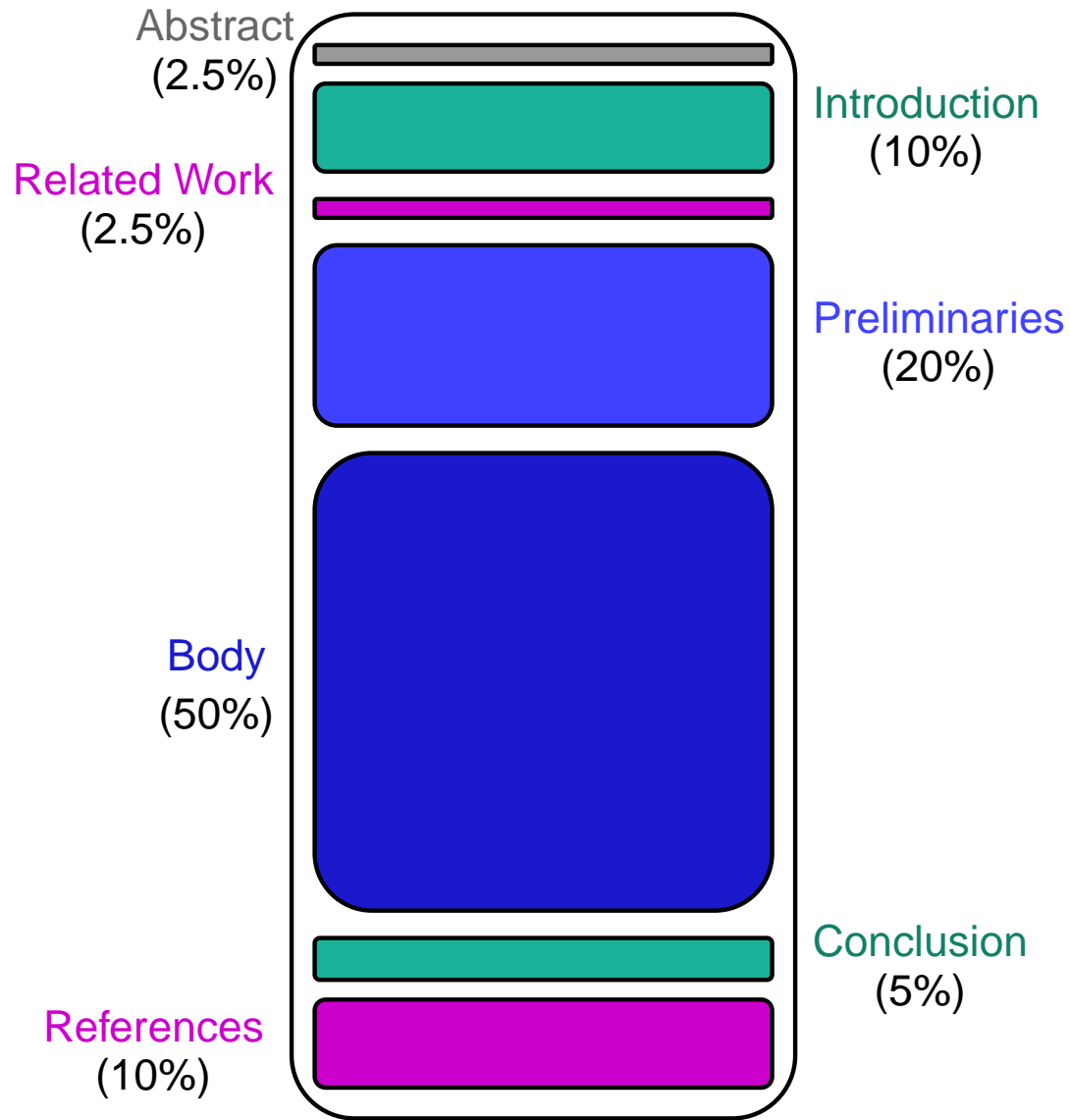
- Review:** Yes, high threshold (international experts are reviewing)
- Goal:** Survey or complete work on a topic (in-depth paper)
- Size :** From 20 pages up to 70
- Freshness:** About one year

# Structure of Scientific Papers

A typical scientific paper has the same basic structure as project reports (familiar to students from this university):

- Abstract
- Introduction
- Related work
- Preliminaries
- Main part
- Conclusion
- Bibliography
- Appendices

# Structure of Scientific Papers



# First Read Through (Step 1)

## 1. Read:

- Abstract
- Introduction
- Related Work
- Conclusion
- References (Only those mentioned in one of the previous sections)

## 2. Reply to the following questions:

- Which research community is the paper addressing ? [Introduction, Related Work]
- What are the contributions of the paper (according to the authors) ? [Abstract, Introduction, Conclusion]
- What are the possible implications of the contributions ? (direct applications, new techniques, new fields, . . . ) [Introduction]

# First Read Through (Step 2)

## 1. Read:

- **Preliminaries** (Identify the notations or analysis methods)
- **Body** (**Warning !** Do **NOT** read the proofs or experiment settings)

## 2. Reply to the following questions:

- **If I assume that the proofs are underlinecorrect or the experimental setting and the analysis method relevant, do the authors meet the list of contributions ?** [Preliminaries, Body]
  - **Yes:** Go to “In-depth Read Through”
  - **No:** Go over the paper again or ask your supervisor for help

# In-depth Read Through

## 1. Read:

- **Body** (Everything)
- **References** (Quick glance at external theorems/experiments)

## 2. Last Tips:

- **A proof/experiment is too technical, I do not understand it!**
  - Is it relevant to understand it ?
    - Yes: Try harder or contact your supervisor
    - No: Skip it!
- **I found an error !**
  - Are you sure ?
    - Double check
    - Triple check
    - Ask your advisor
  - Do the contributions of the paper still hold ?
    - Yes: Then it is not so important
    - No: Write a paper!

# Looking at References

**A paper is just one link in a chain !**

**Don't stop once you have read it, it's only the beginning !**

**Looking at references allow you to:**

- Discover the community around it
- Understand the context
- Put the paper in perspective
- Link it with other fields/topics

# CiteSeer – A Tool for You

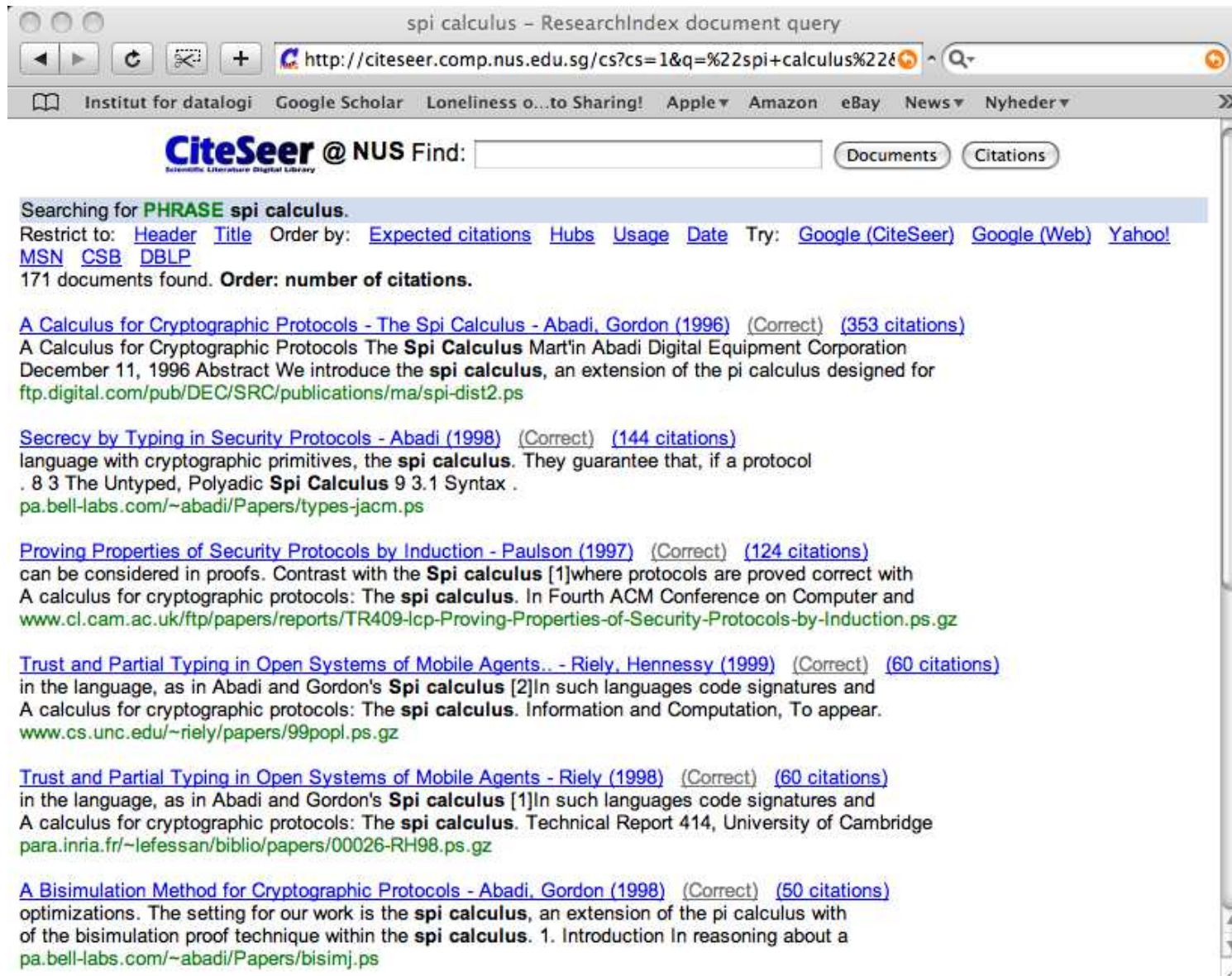


The screenshot shows a web browser window with the following elements:

- Browser Title Bar:** Computer and Information Science Papers CiteSeer Publications ResearchIndex
- Address Bar:** <http://citeseer.comp.nus.edu.sg/cs>
- Search Bar:** Google
- Navigation Bar:** Institut for datalogi, Google Scholar, Apple, Amazon, eBay, News, Nyheder, jensunmack.dk, Datalogi
- Logo:** CiteSeer.IST Scientific Literature Digital Library @ NUS National University of Singapore
- Navigation Tabs:** Documents (selected), Citations
- Search Form:** A text input field followed by a "Search Documents" button.
- Text:** Documents indexed by CiteSeer.IST at NUS
- Links:** [Submit Documents](#) | [Statistics](#) | [Help](#) | [CiteSeer Metadata](#) | [New! Announcements](#)  
Copyright [NEC](#) and [Penn State](#) | [Privacy Policy](#) | [About](#) | [Feedback](#)
- Status:** Searching 767558 documents.
- Footer:** Hosted by National University of Singapore's [School of Computing](#)



# CiteSeer – Result of our Request



The screenshot shows a web browser window with the address bar containing the URL `http://citeseer.comp.nus.edu.sg/cs?cs=1&q=%22spi+calculus%22&`. The browser's address bar also shows the text "spi calculus - ResearchIndex document query". The browser's search bar contains the text "spi calculus". The browser's search bar also shows the text "spi calculus". The browser's search bar also shows the text "spi calculus".

**CiteSeer @ NUS** Find:  Documents Citations

Searching for **PHRASE** spi calculus.

Restrict to: [Header](#) [Title](#) Order by: [Expected citations](#) [Hubs](#) [Usage](#) [Date](#) Try: [Google \(CiteSeer\)](#) [Google \(Web\)](#) [Yahoo!](#) [MSN](#) [CSB](#) [DBLP](#)

171 documents found. **Order: number of citations.**

[A Calculus for Cryptographic Protocols - The Spi Calculus - Abadi, Gordon \(1996\)](#) (Correct) (353 citations)  
A Calculus for Cryptographic Protocols The **Spi Calculus** Mart'in Abadi Digital Equipment Corporation  
December 11, 1996 Abstract We introduce the **spi calculus**, an extension of the pi calculus designed for  
<ftp.digital.com/pub/DEC/SRC/publications/ma/spi-dist2.ps>

[Secrecy by Typing in Security Protocols - Abadi \(1998\)](#) (Correct) (144 citations)  
language with cryptographic primitives, the **spi calculus**. They guarantee that, if a protocol  
. 8 3 The Untyped, Polyadic **Spi Calculus** 9 3.1 Syntax .  
<pa.bell-labs.com/~abadi/Papers/types-jacm.ps>

[Proving Properties of Security Protocols by Induction - Paulson \(1997\)](#) (Correct) (124 citations)  
can be considered in proofs. Contrast with the **Spi calculus** [1]where protocols are proved correct with  
A calculus for cryptographic protocols: The **spi calculus**. In Fourth ACM Conference on Computer and  
<www.cl.cam.ac.uk/ftp/papers/reports/TR409-lcp-Proving-Properties-of-Security-Protocols-by-Induction.ps.gz>

[Trust and Partial Typing in Open Systems of Mobile Agents... - Riely, Hennessy \(1999\)](#) (Correct) (60 citations)  
in the language, as in Abadi and Gordon's **Spi calculus** [2]In such languages code signatures and  
A calculus for cryptographic protocols: The **spi calculus**. Information and Computation, To appear.  
<www.cs.unc.edu/~riely/papers/99popl.ps.gz>

[Trust and Partial Typing in Open Systems of Mobile Agents - Riely \(1998\)](#) (Correct) (60 citations)  
in the language, as in Abadi and Gordon's **Spi calculus** [1]In such languages code signatures and  
A calculus for cryptographic protocols: The **spi calculus**. Technical Report 414, University of Cambridge  
<para.inria.fr/~lefessan/biblio/papers/00026-RH98.ps.gz>

[A Bisimulation Method for Cryptographic Protocols - Abadi, Gordon \(1998\)](#) (Correct) (50 citations)  
optimizations. The setting for our work is the **spi calculus**, an extension of the pi calculus with  
of the bisimulation proof technique within the **spi calculus**. 1. Introduction In reasoning about a  
<pa.bell-labs.com/~abadi/Papers/bisimj.ps>

# CiteSeer – Paper Informations (Top)

Security by Typing in Security Protocols – Abadi (ResearchIndex)

http://citeseer.comp.nus.edu.sg/318576.html

Institut for datalogi Google Scholar Apple Amazon eBay News Nyheder jensunmack.dk Datalogi

**Secrecy by Typing in Security Protocols (1998)** (Make Corrections) (158 citations)  
Martin Abadi

View or download:  
[belllabs.com/~abadi/Pa...typesjacm.ps](#)  
Cached: [PS.gz](#) [PS](#) [PDF](#) [Image](#) [Update](#) [Help](#)

From: [cryptosoft.com/html/secpub](#) (more)  
(Enter author homepages)

**CiteSeer** @ NUS [Home/Search](#) [Context](#) [Related](#)

(Enter summary)

Rate this article: 1 2 3 4 5 (best)  
[Comment on this article](#)

**Abstract:** We develop principles and rules for achieving secrecy properties in security protocols. Our approach is based on traditional classification techniques, and extends those techniques to handle concurrent processes that use shared-key cryptography. The rules have the form of typing rules for a basic concurrent language with cryptographic primitives, the spi calculus. They guarantee that, if a protocol typechecks, then it does not leak its secret inputs. (Update)

**Cited by:** [More](#)  
Secure Composition of Insecure Components - Sewell, Vitek (1999) (Correct)  
Computationally Sound Secrecy Proofs by Mechanized Flow Analysis - Backes, Laud (2006) (Correct)  
A Calculus for Cryptographic Protocols - The Spi Calculus - Abadi, Gordon (1998) (Correct)

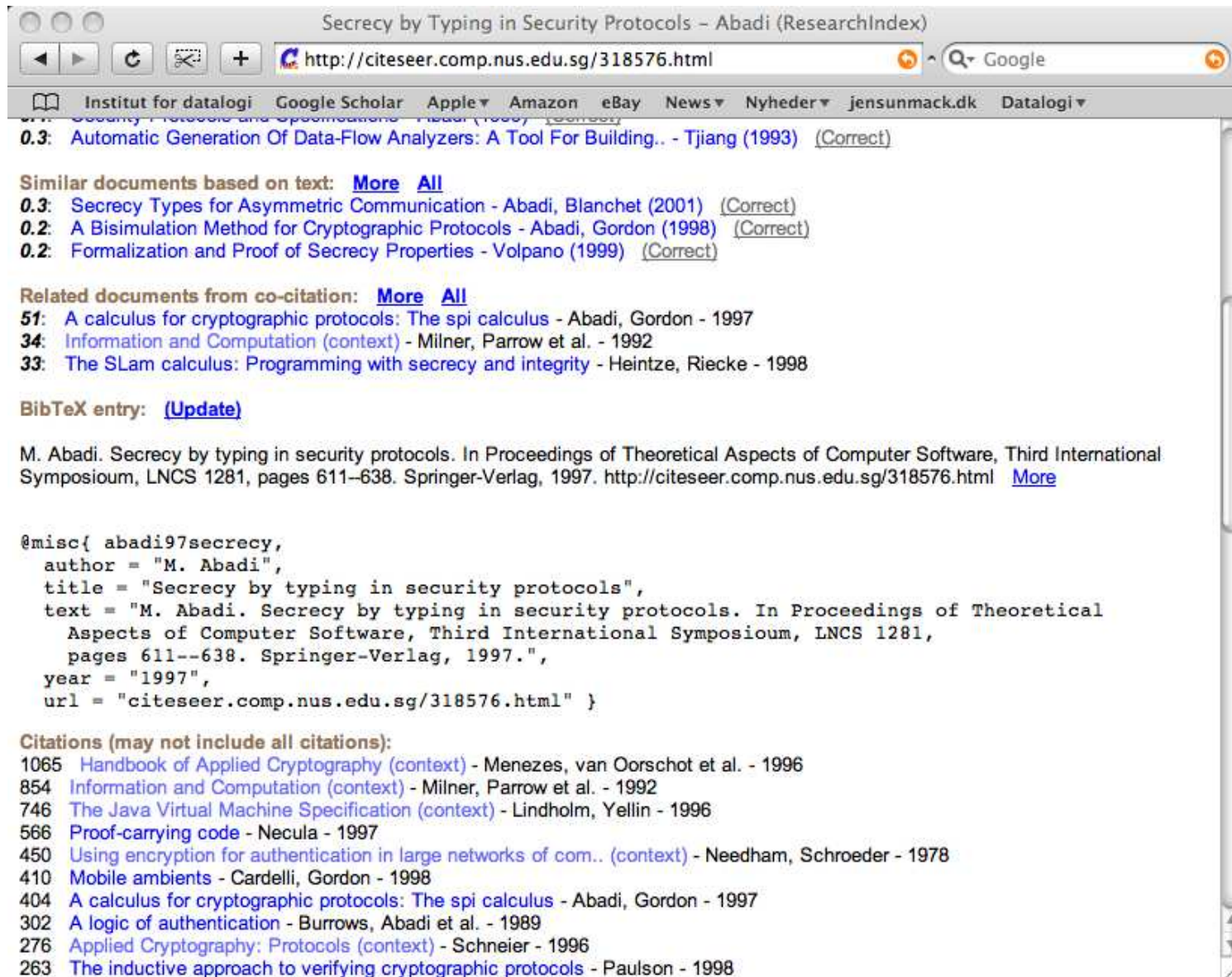
**Similar documents (at the sentence level):**  
**35.0%:** Secrecy by Typing in Security Protocols - Abadi (1997) (Correct)

**Active bibliography (related documents):** [More](#) [All](#)  
**0.4:** Security Protocols and their Properties - Abadi (2000) (Correct)  
**0.4:** Security Protocols and Specifications - Abadi (1999) (Correct)  
**0.3:** Automatic Generation Of Data-Flow Analyzers: A Tool For Building.. - Tjiang (1993) (Correct)

**Similar documents based on text:** [More](#) [All](#)  
**0.3:** Secrecy Types for Asymmetric Communication - Abadi, Blanchet (2001) (Correct)  
**0.2:** A Bisimulation Method for Cryptographic Protocols - Abadi, Gordon (1998) (Correct)  
**0.2:** Formalization and Proof of Secrecy Properties - Volpano (1999) (Correct)

**Related documents from co-citation:** [More](#) [All](#)  
**51:** A calculus for cryptographic protocols: The spi calculus - Abadi, Gordon - 1997  
**34:** Information and Computation (context) - Milner, Parrow et al. - 1992  
**33:** The SLam calculus: Programming with secrecy and integrity - Heintze, Riecke - 1998

# CiteSeer – Paper Informations (Middle)



Security by Typing in Security Protocols – Abadi (ResearchIndex)

http://citeseer.comp.nus.edu.sg/318576.html

Institut for datalogi Google Scholar Apple Amazon eBay News Nyheder jensunmack.dk Datalogi

0.3: Automatic Generation Of Data-Flow Analyzers: A Tool For Building.. - Tjiang (1993) [\(Correct\)](#)

**Similar documents based on text:** [More](#) [All](#)

0.3: Secrecy Types for Asymmetric Communication - Abadi, Blanchet (2001) [\(Correct\)](#)

0.2: A Bisimulation Method for Cryptographic Protocols - Abadi, Gordon (1998) [\(Correct\)](#)

0.2: Formalization and Proof of Secrecy Properties - Volpano (1999) [\(Correct\)](#)

**Related documents from co-citation:** [More](#) [All](#)

51: A calculus for cryptographic protocols: The spi calculus - Abadi, Gordon - 1997

34: Information and Computation (context) - Milner, Parrow et al. - 1992

33: The SLam calculus: Programming with secrecy and integrity - Heintze, Riecke - 1998

**BibTeX entry:** [\(Update\)](#)

M. Abadi. Secrecy by typing in security protocols. In Proceedings of Theoretical Aspects of Computer Software, Third International Symposium, LNCS 1281, pages 611–638. Springer-Verlag, 1997. <http://citeseer.comp.nus.edu.sg/318576.html> [More](#)

```
@misc{ abadi97secrecy,
  author = "M. Abadi",
  title = "Secrecy by typing in security protocols",
  text = "M. Abadi. Secrecy by typing in security protocols. In Proceedings of Theoretical
    Aspects of Computer Software, Third International Symposium, LNCS 1281,
    pages 611--638. Springer-Verlag, 1997.",
  year = "1997",
  url = "citeseer.comp.nus.edu.sg/318576.html" }
```

**Citations (may not include all citations):**

1065 Handbook of Applied Cryptography (context) - Menezes, van Oorschot et al. - 1996

854 Information and Computation (context) - Milner, Parrow et al. - 1992

746 The Java Virtual Machine Specification (context) - Lindholm, Yellin - 1996

566 Proof-carrying code - Necula - 1997

450 Using encryption for authentication in large networks of com.. (context) - Needham, Schroeder - 1978

410 Mobile ambients - Cardelli, Gordon - 1998

404 A calculus for cryptographic protocols: The spi calculus - Abadi, Gordon - 1997

302 A logic of authentication - Burrows, Abadi et al. - 1989

276 Applied Cryptography: Protocols (context) - Schneier - 1996

263 The inductive approach to verifying cryptographic protocols - Paulson - 1998

# CiteSeer – Papers Informations (Bottom)

Secrecy by Typing in Security Protocols – Abadi (ResearchIndex)

http://citeseer.comp.nus.edu.sg/318576.html

Institut for datalogi Google Scholar Apple Amazon eBay News Nyheder jensunmack.dk Datalogi

- 29 Protection in programming-language translations - Abadi - 1990
- 28 National Bureau of Standards - standard, Inform et al. - 1977
- 18 Journal of Functional Programming (context) - rbk, Palsberg et al. - 1997
- 18 A lesson in authentication protocol design - Woo, Lam - 1994
- 15 Proving trust in systems of second-order processes (context) - Dam - 1998
- 13 Limitations on design principles for public key protocols - Syverson - 1996
- 11 Undergraduate lecture notes (context) - Milner, -calculus - 1995
- 7 Control flow analysis for the #-calculus (context) - Bodei, Degano et al. - 1998
- 6 Van Nostrand Reinhold Company Inc (context) - Gasser, Computer - 1988
- 6 Strategies against replay attacks - Aura - 1997
- 3 Private communication (context) - Milner, Pierce - 1997
- 3 Private communication (context) - Gay - 1997

Year of Publication of Citing Articles

Year	Number of Citations
1997	2
1998	12
1999	23
2000	22
2001	19
2002	25
2003	12
2004	6
2005	2
2006	2

The graph only includes citing articles where the year of publication is known.

Documents on the same site (<http://www.cryptosoft.com/html/secpub.htm>): [More](#)

[A New Approach for Delegation Using Hierarchical Delegation.. - Ding, Petersen \(1995\) \(Correct\)](#)

[A Uniform-Complexity Treatment of Encryption and Zero-Knowledge - Goldreich \(1991\) \(Correct\)](#)

[On Signature Schemes With Threshold Verification Detecting.. - Petersen, Michels \(1997\) \(Correct\)](#)

[Online articles have much greater impact](#) [More about CiteSeer.IST at NUS](#) [Add search form to your site](#) [Submit documents](#)  
[Feedback](#)

CiteSeer.IST at NUS - Copyright [Penn State](#) and [NEC](#). Hosted by the [School of Computing, National University of Singapore](#).

# IEEEXplorer – Other Community, Other Tool

The screenshot shows the IEEE Xplore website interface within a browser window. The browser's address bar displays the URL `http://ieeexplore.ieee.org/Xplore/dynhome.jsp`. The browser's search bar contains the text "Google". The browser's bookmark bar includes links to "Institut for datalogi", "Google Scholar", "Apple", "Amazon", "eBay", "News", "Nyheder", "jensunmack.dk", and "Datalogi".

The website header features the "IEEE Xplore" logo with "RELEASE 2.5" below it, and a navigation menu with links for "Home", "Login", "Logout", "Access Information", "Alerts", "Purchase History", "Cart", "Sitemap", and "Help". A secondary navigation bar includes "Welcome Aalborg Universitetsbibliotek" and the IEEE logo. A status bar indicates "1,828,380 documents online" and provides navigation options: "BROWSE", "SEARCH", "IEEE XPLORE GUIDE", and "SUPPORT".

The main content area is divided into several sections:

- Welcome to IEEE Xplore**: A section with a vertical image strip on the left and text stating "... delivering full text access to the world's highest quality technical literature in electrical engineering, computer science, and electronics."
- Browse**: A section with a list of links: "Journals & Magazines", "Conference Proceedings", "Standards", "Books", "Educational Courses", and "Technology Surveys".
- Basic Search**: A section with a search input field, a search button, and a list of search options: "Advanced Search", "Author Search", and "CrossRef Search".

Below the main content area, there are four promotional boxes:

- Content Updates**: "Browse the latest update to see recently added content." with a link to "Latest Content Update".
- Top 100 Documents**: "Find out the most accessed documents for the month." with a link to "View Top 100".
- IEEE Peer Review**: "Publishing the highest quality technical literature" with a link to "Find out more".
- Alerts**: "Register and access your alerts." with a link to "Visit Alerts".

Additional features include a "scitopia.org" search box, an "IEEE Spectrum Magazine" link, and a "SPECTRUM ONLINE" logo with the tagline "Tomorrow's Technology Today".

The footer contains a "Cookies Enabled" notification, a "Help" link, and contact information: "Contact Us", "Privacy & Security", and "IEEE.org". It also includes the text "Indexed by Inspec" and "© Copyright 2008 IEEE – All Rights Reserved".

# Evaluating Scientific Papers

## Ok, I have:

- Read the paper,
- Understood it,
- Browsed the references.

## What's next ?

- List the strength/weakness of the paper (be critical !)
- Define the contributions of the paper (look at the papers quoting it)
- Put the paper in perspective (impact on the community)
- **Make your own opinion !!!!** (very important)

# Summary: How to Read a Paper?

## 1. First Read Through

(Abstract, Introduction, Related Work, Conclusion, References)

Extract the context and the intended contributions

## 2. In Depth Read Through

(Preliminaries, Body, References)

Grab the details

## 3. Looking at References

(References, Citeseer)

Make the link with other papers, look at the real impact

## 4. Evaluate the Paper

(Everything)

Forge your opinion

## 5. Start to Prepare your Presentation

# **Appendices:**

## **How to Read Technical Parts**



# How to Read a Proof

## 1. Analyze the Theorem

- What are the hypothesis ?
- What is the result ?

## 2. Understand the Structure of the Proof

- What type of Proof is it?
  - Direct Proof
  - Proof by Contradiction
  - Proof by Induction
  - Case by case Enumeration
  - Others...
- Decompose the Proof (divide and conquer)
  - Look for Independent Parts (lemmas, propositions, ...)
  - Look for External Theorems (look at [References](#))

## 3. Assume intermediate steps to be true and understand the skeleton of the proof

## 4. If necessary, look at the small annoying steps

# How to Read an Experimental Result

## ● Identify:

1. The setting of the experiment  
(processor, RAM, layout of the network, ...)
2. What concrete parameters are measured  
(computational time, memory used, bandwidth, ...)
3. The method used to analyse the results  
(bare results, average, other statistical methods, ...)
4. The interpretation of the results done by the authors  
(making a theory that will match the facts)
5. The conclusion of the authors  
(According to the theory made previously, what to do ?)

## ● Look for:

1. A bias in the setting
2. A bias in the method used to analyze results
3. A bias in the interpretation of the results
4. A bias in the reasoning from the interpretation to the conclusions

# **Part II:**

# **Present a Scientific Paper**

# Plan

1. Before Starting
2. Organize your Ideas
  - Introduction
  - Preliminaries
  - Body
  - Technicalities
  - Conclusion
3. Writing slides
4. Speaking
5. The presentation
6. One last piece of advice
7. Next Week

# Before Starting

- **Know your Topic**

(Be sure you have understood the paper)

- **Know Your Audience**

(Your talk must take the audience into account)

- **Know Your Goals**

(What are the expectations of the audience ?)

- **Know Your Limits**

(how much time will be needed ?)

# Organize Your Ideas (1/3)

- **Speak about Key Ideas**

(Make sure that all the key ideas of the paper are in your talk)

- **Don't Get Bogged Down in Details**

(Ignore the superfluous and focus the essential)

- **Use A Top-Down Approach**

(starting wide, finishing narrow)

- **Structure Your Talk**

(Make appear several distinct parts in your talk:

Introduction, Preliminaries, Body, Technicalities, Conclusion)

# Organize Your Ideas (2/3)

## Introduction

- Define the problem
- Motivate the audience
- Discuss earlier/posterior Work
- Emphase the contribution of the paper
- Provide a road-map

## Preliminaries

- Introduce terminology and notations or the setting of the experiment
- Redefine the problem more technically
- “Definition by example” can be a valid strategy, if the talk is short and there are many definitions.

# Organize Your Ideas (3/3)

## Body

- Present the main results
- Explain the meaning of the results
- Give some Examples

## Technicalities

- Either sketch the proof of an important result or present some experimental results

## Conclusion

- Recapitulate the main results
- Give your opinions on the paper
- Indicate that your talk is over



# Writing slides

- **Use a computer!**

(use computers: PowerPoint, LaTeX, OpenOffice, ...)

- **Simpler is better !**

(do not overload the content. the frame or the background of your slides)

- **Use colours !**

(but please do not **exaggerate !**)

- **... and pictures**

(one picture is worth a thousand words)

- **One slide = 2 minutes (average)**

(think about timing)

# Speaking to an audience

- **Rehearse at least once**

(mentally is ok, but speaking at loud voice is better)

- **Find the right words**

(prepare some full sentences to say during the talk)

- **transitions are the keys !**

(prepare transition between slides)

- **Learn to improvise**

(whatever you do, you will have to improvise)

- **Humour is OK !**

(but try to be funny !)

# The Show

- **Vary your intonation**  
(avoid speaking in a monotone voice)
- **Get your audience to participate**
- **Maintain eye contact**  
(don't show them your back)
- **Careful where you stand!**  
(don't hide the slides)
- **Do not overrun**  
(do not forget the time)
- **I make a mistake ... but the show must go on**  
(do not stop to correct small mistakes – you may lose your way in the details)

# One last piece of advice

Practice!

Practice !

Practice !

Practice !

**Practice !**

# Next Week

**Let's get started !**

Two volunteers required to present and Two opponents for two papers.

The presentations should be no longer than 45 minutes each.