



Literature Research in Computer Science

Martin Byrenheid & Paul Walther
Chair of Privacy and Data Security

Goals

1. Gather and understand existing knowledge and solutions
 - Avoid re-inventing the wheel
 - Avoid making the same mistakes

Goals

1. Gather and understand existing knowledge and solutions
 - Avoid re-inventing the wheel
 - Avoid making the same mistakes
2. Identify open problems and limitations of existing solutions

Goals

1. Gather and understand existing knowledge and solutions
 - Avoid re-inventing the wheel
 - Avoid making the same mistakes
2. Identify open problems and limitations of existing solutions
3. Learn about related research community
 - Common vocabulary
 - Established scientific methods
 - Preferred venues for scientific discourse

Goals

1. Gather and understand existing knowledge and solutions
 - Avoid re-inventing the wheel
 - Avoid making the same mistakes
2. Identify open problems and limitations of existing solutions
3. Learn about related research community
 - Common vocabulary
 - Established scientific methods
 - Preferred venues for scientific discourse

In the following:

Goals

1. Gather and understand existing knowledge and solutions
 - Avoid re-inventing the wheel
 - Avoid making the same mistakes
2. Identify open problems and limitations of existing solutions
3. Learn about related research community
 - Common vocabulary
 - Established scientific methods
 - Preferred venues for scientific discourse

In the following:

- Methods for efficient *searching* for relevant scientific literature

Goals

1. Gather and understand existing knowledge and solutions
 - Avoid re-inventing the wheel
 - Avoid making the same mistakes
2. Identify open problems and limitations of existing solutions
3. Learn about related research community
 - Common vocabulary
 - Established scientific methods
 - Preferred venues for scientific discourse

In the following:

- Methods for efficient *searching* for relevant scientific literature
- Methods for efficient *reading* of scientific literature

Scientific literature

- Conference proceedings
 - Published once a year
 - Typically between 10 and 18 pages without references
 - Results have been presented at scientific conference
- Journals
 - Published bi-monthly
 - Typically between 12 and 28 pages without references
 - May be extended version of a conference publication

Search engines for scientific literature

- Google scholar
- DBLP computer science bibliography
- ACM digital library
- Springer Link
- IEEE Xplore

Google Scholar

IEEE Xplore®

ACM DL DIGITAL LIBRARY



Search engines for scientific literature

- Google scholar
 - DBLP computer science bibliography
 - ACM digital library
 - Springer Link
 - IEEE Xplore
- Keyword search**
- Research groups may use different vocabulary → be creative!
 - Add “survey”, “systematization of knowledge” (SoK) or “state of” to find summaries
 - Use keywords from previously found papers
 - Use filtering mechanisms (e.g. year)

Google Scholar

IEEE Xplore®

ACM DL DIGITAL LIBRARY



Efficient searching

New directions in cryptography

W Diffie, M Hellman - IEEE transactions on Information Theory, 1976 - ieeexplore.ieee.org

Two kinds of contemporary developments in **cryptography** are examined. Widening applications of teleprocessing have given rise to a need for **new** types of cryptographic systems, which minimize the need for secure key distribution channels and supply the ...

☆ 99 Cited by 18941 Related articles All 153 versions

Efficient searching

title

New directions in cryptography

W Diffie, M Hellman - IEEE transactions on Information Theory, 1976 - ieeexplore.ieee.org

Two kinds of contemporary developments in **cryptography** are examined. Widening applications of teleprocessing have given rise to a need for **new** types of cryptographic systems, which minimize the need for secure key distribution channels and supply the ...

☆ 🔖 Cited by 18941 Related articles All 153 versions

Efficient searching

author list

title

New directions in cryptography

W Diffie, M Hellman - IEEE transactions on Information Theory, 1976 - ieeexplore.ieee.org

Two kinds of contemporary developments in **cryptography** are examined. Widening applications of teleprocessing have given rise to a need for **new** types of cryptographic systems, which minimize the need for secure key distribution channels and supply the ...

☆ 🔗 Cited by 18941 Related articles All 153 versions

A diagram illustrating search annotations on a search result. A red arrow labeled 'author list' points to the authors 'W Diffie, M Hellman'. Another red arrow labeled 'title' points to the title 'New directions in cryptography'. The title and authors are enclosed in a red rectangular box.

Efficient searching

author list title publication venue

New directions in cryptography 1976 - ieeexplore.ieee.org

W Diffie, M Hellman - IEEE transactions on Information Theory

Two kinds of contemporary developments in **cryptography** are examined. Widening applications of teleprocessing have given rise to a need for **new** types of cryptographic systems, which minimize the need for secure key distribution channels and supply the ...

☆ 🔗 Cited by 18941 Related articles All 153 versions



Efficient searching

author list title publication venue year of publication

New directions in cryptography
W Diffie, M Hellman - IEEE transactions on Information Theory 1976 - ieeexplore.ieee.org

Two kinds of contemporary developments in **cryptography** are examined. Widening applications of teleprocessing have given rise to a need for **new** types of cryptographic systems, which minimize the need for secure key distribution channels and supply the ...

☆ 99 Cited by 18941 Related articles All 153 versions



Efficient searching

author list

title

publication venue

year of publication

citation count

New directions in cryptography
W Diffie, M Hellman - IEEE transactions on Information Theory 1976 - ieeexplore.ieee.org

Two kinds of contemporary developments in **cryptography** are examined. Widening applications of teleprocessing have given rise to a need for **new** types of cryptographic systems, which minimize the need for secure key distribution channels and supply the ...

☆ ⓘ Cited by 18941 Related articles All 153 versions

Efficient searching

The image shows a search result snippet with several fields highlighted in red boxes and labeled with red arrows:

- author list**: Points to the box containing "W Diffie, M Hellman".
- title**: Points to the box containing "New directions in cryptography".
- publication venue**: Points to the box containing "IEEE transactions on Information Theory".
- year of publication**: Points to the box containing "1976".
- citation count**: Points to the box containing "Cited by 18941".

The search result text is as follows:

New directions in cryptography
W Diffie, M Hellman - IEEE transactions on Information Theory 1976 - ieexplore.ieee.org
Two kinds of contemporary developments in **cryptography** are examined. Widening applications of teleprocessing have given rise to a need for **new** types of cryptographic systems, which minimize the need for secure key distribution channels and supply the ...
☆ ⓘ Cited by 18941 Related articles All 153 versions

- Look for papers with promising titles

Efficient searching



- Look for papers with promising titles
- Use literature management tools
 - Zotero, JabRef, Citavi, Mendeley, etc.
 - Provide plugins for automatic import

Efficient searching



- Look for papers with promising titles
- Use literature management tools
 - Zotero, JabRef, Citavi, Mendeley, etc.
 - Provide plugins for automatic import
- Perform searching and reading separately

Efficient searching

[PDF] **Traffic Morphing: An Efficient Defense Against Statistical Traffic Analysis.**

[CV Wright](#), [SE Coull](#), [F Monrose](#) - NDSS, 2009 - Citeseer

Recent work has shown that properties of network **traffic** that remain observable after encryption, namely packet sizes and timing, can reveal surprising information about the **traffic's** contents (eg, the language of a VoIP call [29], passwords in secure shell logins [20] ...

☆  Cited by 293 Related articles All 18 versions 

- Forward search
 - Provided by Google Scholar and IEEE Xplore
 - Combined with filtering by year helps to identify most recent works

Efficient searching

[PDF] [Traffic Morphing: An Efficient Defense Against Statistical Traffic Analysis.](#)

[CV Wright](#), [SE Coull](#), [F Monroe](#) - NDSS, 2009 - Citeseer

Recent work has shown that properties of network **traffic** that remain observable after encryption, namely packet sizes and timing, can reveal surprising information about the **traffic's** contents (eg, the language of a VoIP call [29], passwords in secure shell logins [20] ...

☆  **Cited by 293** [Related articles](#) [All 18 versions](#) 

- Forward search
 - Provided by Google Scholar and IEEE Xplore
 - Combined with filtering by year helps to identify most recent works

Efficient searching

[PDF] **Traffic Morphing: An Efficient Defense Against Statistical Traffic Analysis.**

[CV Wright](#), [SE Coull](#), [F Monrose](#) **NDSS, 2009** [Citeseer](#)

Recent work has shown that properties of network **traffic** that remain observable after encryption, namely packet sizes and timing, can reveal surprising information about the **traffic's** contents (eg, the language of a VoIP call [29], passwords in secure shell logins [20] ...

☆ [🔗](#) Cited by 293 [Related articles](#) [All 18 versions](#) [↔](#)

- Forward search
 - Provided by Google Scholar and IEEE Xplore
 - Combined with filtering by year helps to identify most recent works
- Check publication venue
 - Conference websites typically have an “accepted papers” section
 - You can also find the list of accepted papers on DBLP or IEEE Xplore
 - “Proceedings” usually indicates conference
 - “Transactions” usually indicates journals

Efficient searching

[PDF] **Traffic Morphing: An Efficient Defense Against Statistical Traffic Analysis.**

CV Wright, SE Coull, F Monroe - NDSS, 2009 - Citeseer

Recent work has shown that properties of network **traffic** that remain observable after encryption, namely packet sizes and timing, can reveal surprising information about the **traffic's** contents (eg, the language of a VoIP call [29], passwords in secure shell logins [20] ...

☆ 99 Cited by 293 Related articles All 18 versions ⇨⇨

- Check authors to identify research groups
 - Research group websites typically contain a list of recent publications
 - Check if these groups are still active

Forward & backward search

- Papers cite previous work
→ backward search
- Papers get cited by later work
→ forward search
- Citation graph
- Tool assistance:
connectedpapers.com, inciteful.xyz, semanticscholar.org

Reading papers



Reading papers



- Prioritization

- Title
- Number of citations
- Ranking of venue
- Year of publication

Reading papers



- Prioritization

- Title
 - Number of citations
 - Ranking of venue
 - Year of publication
-
- Older papers with a high number of citations might be milestone papers or particularly controversial
 - Publication venue indicates quality of work

Reading papers

- Peer-review is common to all scientific conferences and journals
- Platforms like arXiv and the IACR ePrint archive do not require peer-review
- Commonly used indicator for quality of venue: rankings

Reading papers

- Peer-review is common to all scientific conferences and journals
- Platforms like arXiv and the IACR ePrint archive do not require peer-review
- Commonly used indicator for quality of venue: rankings

CORE ranking

- A* - flagship conference, a leading venue in a discipline area
- A - excellent conference, and highly respected in a discipline area
- B - good conference, and well regarded in a discipline area
- C - other ranked conference venues that meet minimum standards

Reading papers

- Peer-review is common to all scientific conferences and journals
- Platforms like arXiv and the IACR ePrint archive do not require peer-review
- Commonly used indicator for quality of venue: rankings

CORE ranking

- A* - flagship conference, a leading venue in a discipline area
- A - excellent conference, and highly respected in a discipline area
- B - good conference, and well regarded in a discipline area
- C - other ranked conference venues that meet minimum standards

Microsoft Academic

- Provides fine-grained ranking by citations, prestige etc.

Reading papers

Three-pass approach by S. Keshav

- **First pass:** Get a general idea about the paper
- **Second pass:** Grasp the paper's content, but not its details
- **Third pass:** Understand the paper in depth

Reading papers

Three-pass approach by S. Keshav

- **First pass:** Get a general idea about the paper
- **Second pass:** Grasp the paper's content, but not its details
- **Third pass:** Understand the paper in depth → not needed for literature survey

Reading papers

First pass

1. Carefully read abstract, introduction and conclusion
2. Read the section and sub-section headings, ignore everything else

Reading papers

First pass

1. Carefully read abstract, introduction and conclusion
2. Read the section and sub-section headings, ignore everything else

Goal: Answering the following questions:

1. *Context:* Which problem/question does it address? Which other papers is it related to?
2. *Contributions:* What are the paper's main contributions? Does it improve an existing solution or present a completely novel approach?
3. *Category:* What type of paper is this? (e.g. measurement, theory, survey)
4. *Clarity:* Is the paper well-written?

Reading papers

- Note down your answers and thoughts regarding the aforementioned questions
- Use your own words instead of copying text passages from the paper
- Decide if paper is still relevant → keep notes even if it is irrelevant
- Include yet unknown related papers in your literature research

Reading papers

Second pass

- Read other paper sections, but ignore details such as proofs

Reading papers

Second pass

- Read other paper sections, but ignore details such as proofs

Goals:

- Grasping the content of the paper
- Summarize the main thrust of the paper, with supporting evidence
- Identify relevant references for further literature search

Reading papers

Second pass

- Read other paper sections, but ignore details such as proofs

Goals:

- Grasping the content of the paper
- Summarize the main thrust of the paper, with supporting evidence
- Identify relevant references for further literature search

- While reading, write a short summary of the paper in your own words
- Note down open questions or doubts about the paper → discuss them with your supervisor
- Use insights from reading and from related work section to guide literature search (backward search)

Further recommendations

- Before and during your literature research, think about how you would approach the topic
- Note down questions that come up and actively try to answer them with your research
- Think about what properties an ideal solution to a security problem should have
- Do not underestimate the effort required to read papers and their relation to the bigger picture

Summary

- Scientific discourse via conferences and journals
- Search techniques
 - Keyword search
 - Forward search
 - Backward search
 - Conference/Journal/Research group websites
- Conference/journal rankings can be used for prioritization
- Three-pass reading can be used to avoid wasting time with irrelevant papers
- Read actively by focusing on specific questions
- Keep notes and write summaries of what you read
 - Avoid copying text from the paper

Further reading I

- [1] Wayne C Booth, Gregory G Colomb, and Joseph M Williams. *The craft of research*. University of Chicago press, 2003.
- [2] Justin Zobel. *Writing for computer science*. Vol. 8. Springer, 2004.
- [3] Srinivasan Keshav. „How to read a paper“. In: *ACM SIGCOMM Computer Communication Review* 37.3 (2007), pp. 83–84.
- [4] *Microsoft Academic*. URL: <https://academic.microsoft.com/conferences> (visited on 04/10/2020).
- [5] *CORE Conference Portal*. URL: <http://portal.core.edu.au/conf-ranks/> (visited on 04/10/2020).