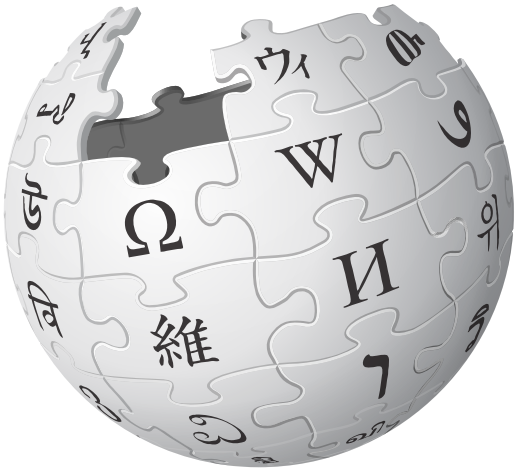
The commons, the open access movement, and the Dissemin platform

Pablo Rauzy
pablo.rauzy@univ-paris8.fr
https://pablo.rauzy.name/

UNIVERSITÉ PARIS 8 VINCENNES-SAINT-DENIS

19th January, 2017 @ Moulis
Seminar @ Station for Theoretical and Experimental Ecology



WIKIPEDIA

WIKIP€DIA

WIKIP€DIA

- Anyone can contribute new entries.
- Anyone can improve existing entries.

WIKIP€DIA

- Anyone can contribute new entries.
- Anyone can improve existing entries.
- Only 30€ to access an entry (even the long ones!)

WIKIP€DIA

- Anyone can contribute new entries.
- Anyone can improve existing entries.
- Only 30€ to access an entry (even the long ones!)
- Yearly subscriptions:

INDIVIDUAL	1000 €	3 entries/day
INDIVIDUAL	5000 €	**unlimited** access
ORGANIZATION	50 000 €	5 entries/day/individual
ORGANIZATION	300 000 €	**unlimited** access

Welcome to academia, Neo

Approximative organization of research

1. Looking for a good question.
2. Researching this question.
3. Obtaining results.
4. Writing a paper.
5. Submission of the paper. *preprint*
6. Peer-review of the paper. *postprint*
7. "Publication" of the paper. *published version*

The role of the publishers

- Laying out papers.
- Distributing papers.
- Make money.
- “Publicize” researchers. . .

Public costs, private profits

- Public money funds:
  - people, facilities, material, etc.,
  - quality control,
  - sometimes even publication costs.

Public costs, private profits

- Public money funds:
  - people, facilities, material, etc.,
  - quality control,
  - sometimes even publication costs.

- Then, publishers require copyright to be transfered to them:
  - private appropriation of researchers' productions,
  - sold back to researchers (labs' and universities' libraries),
  - at exorbitant prices.

Costs: example of the ENS Paris (2011)

Service commun de documentation (academic libraries):

- Total spendings: 2 101 587,47 €.
- Including documentary expenses: 1 083 885,16 €.

Costs: example of the ENS Paris (2011)

Service commun de documentation (academic libraries):

- Total spendings: 2 101 587,47 €.
- Including documentary expenses: 1 083 885,16 €.

> « nous rappelons que les publics scientifiques de l'ENS bénéficient en outre des abonnements électroniques acquis par le CNRS au niveau national et mis à disposition via ses portails nationaux. Ceci constitue un **facteur d'économie important** pour certains départements de l'ENS, qui n'acquièrent pas ces ressources sur leurs budgets propres. Il en est de même pour les ressources consultables par les chercheurs de l'ENS auprès d'autres grands établissements parisiens, notamment l'UPMC. »

Costs: example of the CNRS (2013)

- Documentary expenses: ∼36 millions €.

Costs: example of Télécom ParisTech (2009–2014)

- Between 2009 and 2014 at Télécom ParisTech:
  - -55% paper subscriptions,
  - +33% electronic subscriptions.
- In the mean time, subscriptions costs:
  - Reed-Elsevier: +21%,
  - Springer: +32%,
  - IEEE: +61%.

Profits: example of Reed-Elsevier

- 2013:
  - Net revenues: $9.44B
  - Gross profit: $6.13B
- 2014:
  - Net revenues: $9.52B
  - Gross profit: $6.21B
- 2015:
  - Net revenues: $9.13B
  - Gross profit: $5.87B

Liberté, égalité, sororité

- The cost in € is only a symptom, not the real problem.
- Equality among students and researchers throughout the world.
- Citizen access to science.

- The Budapest statement defines open access as follows:

  "By 'open access' to this literature, we mean its **free availability on the public internet**, permitting any users to read, download, copy, distribute, print, search, or link to the full texts of these articles, crawl them for indexing, pass them as data to software, or use them **for any** other **lawful purpose, without financial, legal, or technical barriers** other than those inseparable from gaining access to the internet itself.
  The only constraint on reproduction and distribution, and the only role for copyright in this domain, should be to **give authors control over the integrity of their work and the right to be properly acknowledged and cited**."

There are several ways to open access:

There are several ways to open access:

- *Green OA*:
  - Papers are deposited in those repositories directly by their authors.
  - Repositories (national, institutional, or disciplinary) guarantee long-lasting storage.
  - No peer-reviews, parallel to the "traditional" publication process.

There are several ways to open access:

- *Green OA*:
  - Papers are deposited in those repositories directly by their authors.
  - Repositories (national, institutional, or disciplinary) guarantee long-lasting storage.
  - No peer-reviews, parallel to the "traditional" publication process.
- *Gold OA*:
  - Open access journals or conferences, papers available through the publishers' website.
  - Unfortunately hijacked by lobbies.
  - Nowadays $\approx$ "author pays" OA.

There are several ways to open access:

- *Green OA*:
  - Papers are deposited in those repositories directly by their authors.
  - Repositories (national, institutional, or disciplinary) guarantee long-lasting storage.
  - No peer-reviews, parallel to the "traditional" publication process.
- *Gold OA*:
  - Open access journals or conferences, papers available through the publishers' website.
  - Unfortunately hijacked by lobbies.
  - Nowadays $\approx$ "author pays" OA.
- *Diamond OA*:
  - The goal is to make research results a *knowledge common*.
  - *Libre* open access.
  - Researchers should seize back their means of production.
  - Use free software for infrastructures.

We are living in a transition period.

- The question is: to which OA model?

We are living in a transition period.

- The question is: to which OA model?
- Green OA:

We are living in a transition period.

- The question is: to which OA model?
- Green OA:
  - spurs researchers to become aware of OA;

We are living in a transition period.

- The question is: to which OA model?
- Green OA:
  - spurs researchers to become aware of OA;
  - permits access to research results to everyone as of now;

We are living in a transition period.

- The question is: to which OA model?
- Green OA:
  - spurs researchers to become aware of OA;
  - permits access to research results to everyone as of now;
  - paves the way for Diamond OA models (overlay journals).

We are living in a transition period.

- The question is: to which OA model?
- Green OA:
  - spurs researchers to become aware of OA;
  - permits access to research results to everyone as of now;
  - paves the way for Diamond OA models (overlay journals).
- Obstacles:
  - researchers have doubts about their own rights;
  - arduousness of the deposit operation (hello HAL).

We are living in a transition period.

- The question is: to which OA model?
- Green OA:
  - spurs researchers to become aware of OA;
  - permits access to research results to everyone as of now;
  - paves the way for Diamond OA models (overlay journals).
- Obstacles:
  - researchers have doubts about their own rights;
  - arduousness of the deposit operation (hello HAL).

$\Rightarrow$ The goal of Dissemin is to optimize the number of deposits in OA repositories.

Dissemin helps researchers to deposit their papers in OA repositories.

- For each researchers, Dissemin:
  - lists their papers;
  - informs about the ratio of their papers that:
    - are available in OA;
    - could be available in OA but are not;
    - we don't know the status of;
    - the publisher forbids to upload.
- For each paper, Dissemin:
  - retrieves metadata;
  - offers a direct access to the PDF if their is already an OA version;
  - allows to deposit the paper **in two clicks**.

Demonstration

http://dissem.in/

dissemin Home FAQ Login

dissem.in is currently in public beta. Please, let us know about any issue you might have, either on Github or by email at bugs@dissem.in.

Welcome to dissemin

Dissemin helps researchers ensure that their publications are freely available to their readers. Our free service spots paywalled papers and lets you upload them in one click to Zenodo, an innovative repository backed by the EU.

Still unsure? Read below or check out the FAQ.

Look up a researcher:

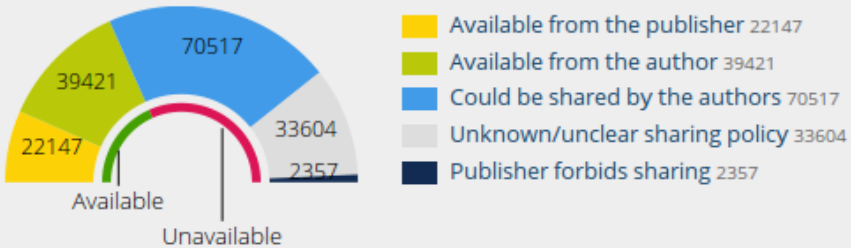
Firstname Lastname Search

or Start with ORCID

Green open access

Many researchers do not use their right to make their papers freely available online, in addition to the paywalled version offered by traditional publishers.

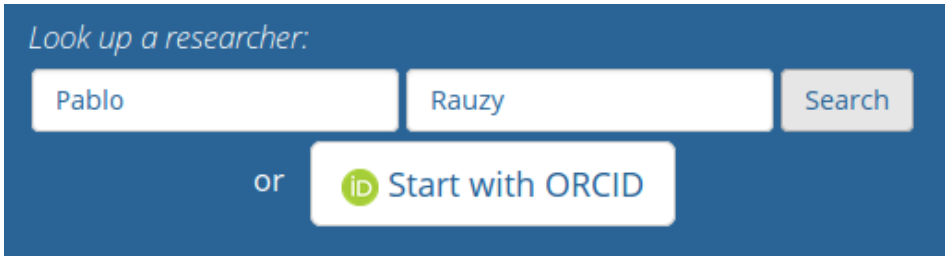
This forces libraries to buy overpriced electronic subscriptions to journals, when they can afford them at all.

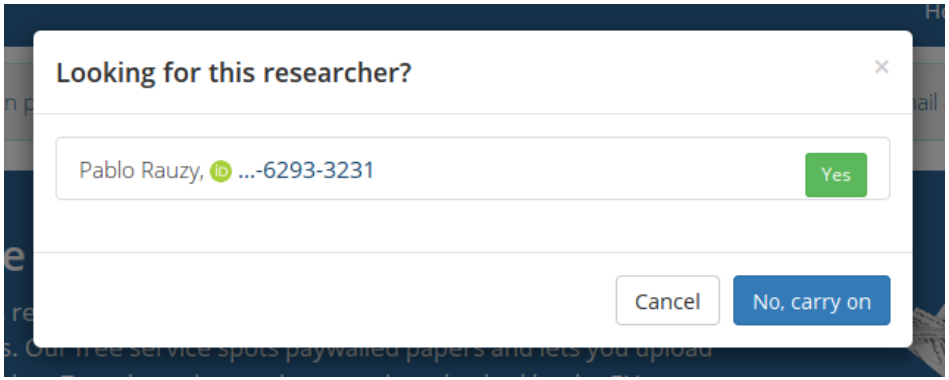


Open repositories

Uploading your papers on your own webpage is not enough. Such copies are less stable and harder to find than documents uploaded to well-indexed repositories.

Dissemin searches for copies of your papers in a large collection of open repositories and tells you which ones cannot be accessed.


Look up a researcher:
Pablo
Rauzy
Search
or
Start with ORCID


Looking for this researcher?
Pablo Rauzy, ...-6293-3231
Yes
Cancel
No, carry on

Papers authored by Pablo Rauzy

2016

Ágnes Kiss, Juliane Krämer, **Pablo Rauzy**, Jean-Pierre Seifert

Algorithmic Countermeasures Against Fault Attacks and Power Analysis for RSA-CRT

Upload | **Springer Verlag**, Lecture Notes in Computer Science, .

2015

Pablo Rauzy, Sylvain Guilley, Zakaria Najm

Formally proved security of assembly code against power analysis: A case study on balanced logic

Download | **Springer Verlag**, Journal of Cryptographic Engineering, **3**(6).

Lionel Riviere, Zakaria Najm, **Pablo Rauzy**, Jean-Luc Danger, Julien Bringer, Laurent Sauvage

High precision fault injections on the instruction cache of ARMv7-M architectures

Download | 2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST).

2014

Pablo Rauzy, Sylvain Guilley

Countermeasures against High-Order Fault-Injection Attacks on CRT-RSA

Download | 2014 Workshop on Fault Diagnosis and Tolerance in Cryptography.

Pablo Rauzy, Sylvain Guilley

Formal Analysis of CRT-RSA Vigilant's Countermeasure Against the

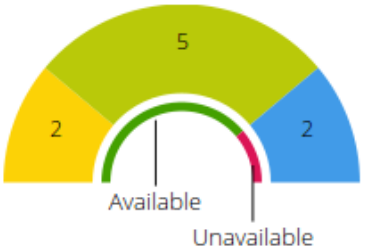
Researcher

Pablo Rauzy

pablo.rauzy.name

0000-0002-6293-3231

9 publications

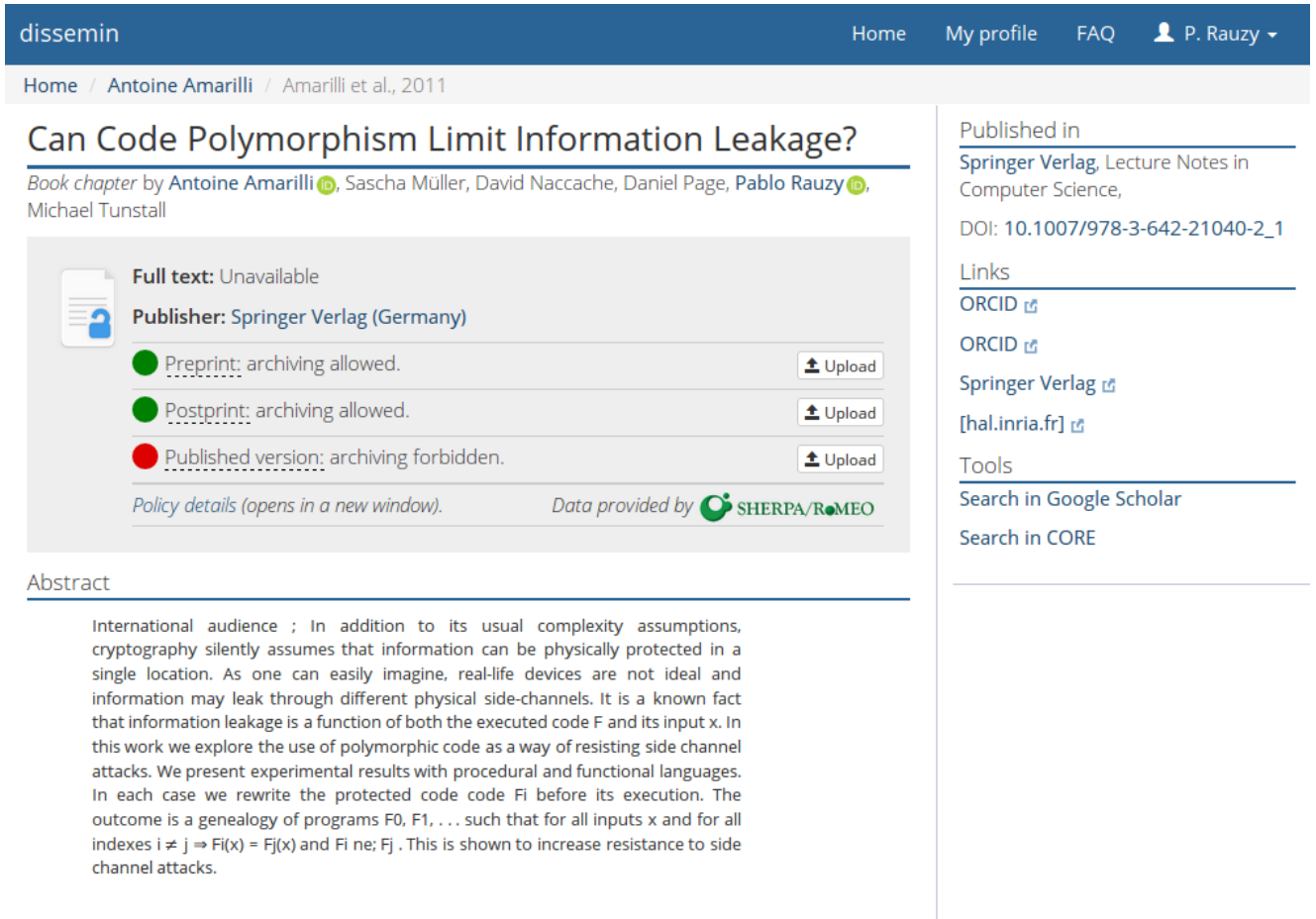


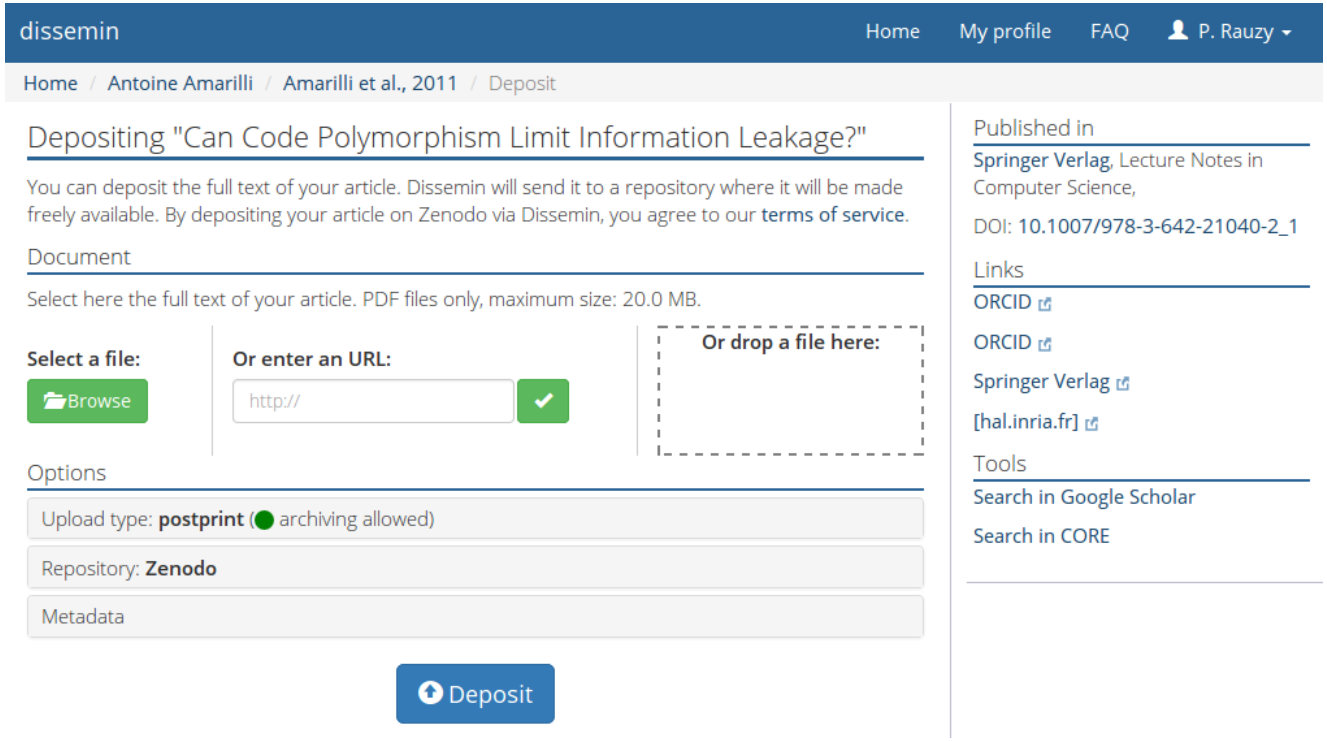
- Available from the publisher 2
- Available from the author 5
- Could be shared by the authors 2
- Unknown/unclear sharing policy 0
- Publisher forbids sharing 0

Refine search

By document type:

- Journal article
- Proceedings article
- Book chapter
- Book
- Journal issue
- Proceedings
- Entry
- Poster
- Report
- Thesis
- Dataset


dissemin
Home
My profile
FAQ
P. Rauzy
Home / Antoine Amarilli / Amarilli et al., 2011
Can Code Polymorphism Limit Information Leakage?
Book chapter by Antoine Amarilli, Sascha Müller, David Naccache, Daniel Page, Pablo Rauzy, Michael Tunstall
Full text: Unavailable
Publisher: Springer Verlag (Germany)
Preprint: archiving allowed.
Upload
Postprint: archiving allowed.
Upload
Published version: archiving forbidden.
Upload
Policy details (opens in a new window).
Data provided by SHERPA/RoMEO
Abstract
International audience ; In addition to its usual complexity assumptions, cryptography silently assumes that information can be physically protected in a single location. As one can easily imagine, real-life devices are not ideal and information may leak through different physical side-channels. It is a known fact that information leakage is a function of both the executed code F and its input x. In this work we explore the use of polymorphic code as a way of resisting side channel attacks. We present experimental results with procedural and functional languages. In each case we rewrite the protected code code Fi before its execution. The outcome is a genealogy of programs F0, F1, . . . such that for all inputs x and for all indexes i ≠ j ⇒ Fi(x) = Fj(x) and Fi ne; Fj . This is shown to increase resistance to side channel attacks.
Published in
Springer Verlag, Lecture Notes in Computer Science,
DOI: 10.1007/978-3-642-21040-2_1
Links
ORCID
ORCID
Springer Verlag
[hal.inria.fr]
Tools
Search in Google Scholar
Search in CORE


dissemin
Home
My profile
FAQ
P. Rauzy
Home / Antoine Amarilli / Amarilli et al., 2011 / Deposit
Depositing "Can Code Polymorphism Limit Information Leakage?"
You can deposit the full text of your article. Dissemin will send it to a repository where it will be made freely available. By depositing your article on Zenodo via Dissemin, you agree to our terms of service.
Document
Select here the full text of your article. PDF files only, maximum size: 20.0 MB.
Select a file:
Browse
Or enter an URL:
http://
Or drop a file here:
Options
Upload type: postprint (archiving allowed)
Repository: Zenodo
Metadata
Deposit
Published in
Springer Verlag, Lecture Notes in Computer Science,
DOI: 10.1007/978-3-642-21040-2_1
Links
ORCID
ORCID
Springer Verlag
[hal.inria.fr]
Tools
Search in Google Scholar
Search in CORE

Options

Upload type:

- Preprint: archiving allowed.
- Postprint: archiving allowed.
- Published version: archiving forbidden.

Policy details (opens in a new window). *Data provided by* SHERPA/RoMEO

Repository:

zenodo — Zenodo is a general-purpose open repository hosted by CERN. If the document does not have a DOI yet, Zenodo will create one.

Metadata

Abstract*

International audience ; In addition to its usual complexity assumptions, cryptography silently assumes that information can be physically protected in a single location. As one can easily imagine, real-life devices are not ideal and information may leak through different physical side-channels. It is a known fact that information leakage is a function of both the executed code F and its input x. In this work we explore the use of polymorphic code as a way of resisting side channel attacks. We present experimental results with procedural and functional languages. In each case we rewrite the protected code code Fi before its execution. The outcome is a genealogy of programs F0, F1, . . . such that for all inputs x and for all indexes i ≠ j ⇒ Fi(x) = Fj(x) and Fi ne; Fj . This is shown to increase resistance to side channel attacks.

License*

- **Creative Commons CCZero**
- **Creative Commons Attribution**
- **Creative Commons Attribution-ShareAlike**
- **Creative Commons Attribution-NonCommercial**
- **Creative Commons Attribution-NoDerivatives**
- **Other open license**

Deposit

Dissemin is a free software.

- Code:
  - `https://github.com/dissemin`,
  - mainly Python (+ HTML, CSS, JavaScript).
- The team:
  - a dozen people (councils, occasional help, communications), all volunteers;
  - development efforts are almost entirely carried by Antonin Delpeuch (pintoch);
  - help is always welcome :).
- Datasources:
  - Primary:
    - CrossRef.org,
    - BASE,
    - SHERPA/RoMEO,
    - Zotero.
  - Secondary (via OAI-PMH):
    - arXiv, HAL, PubMed Central, OpenAIRE, DOAJ, Persée, Cairn.info, Numdam.

Each published paper is assigned a DOI.

- DOI means "*Digital Object Identifier*".
- They are quite practical...
- But are ($\pm$ directly) under the control of publishers.
- So, DOIs point to paywalled version of papers.
- DOAI is an *alternative resolver* which
  - points to an OA version of the paper if possible,
  - or falls back to DOI otherwise.
- To use it, just replace `http://dx.doi.org/` by `http://doai.io/` in links:

`http://dx.doi.org/10.1093/beheco/arw121`
↓
`http://doai.io/10.1093/beheco/arw121`

Open access can also improve Wikipedia!

- As much as possible, Wikipedia articles cite their sources.
- Often these sources are research papers.
- OAbot automatically replaces links to paywalled papers by links to their OA versions.
- OAbot uses CrossRef, BASE, and DOAI's index.

⇒ `https://en.wikipedia.org/wiki/Wikipedia:OABOT`.

Highlights:

- Research results should constitute a *knowledge common* to benefit everyone.
- The transition to OA is a good opportunity to move towards this goal.
- Dissemin helps this transition to Diamond OA by simplifying Green OA.

Questions?