
# Dissemin : simplifier la libération des résultats de la recherche

http://dissem.in/ — @disseminOA

Pablo Rauzy

îledeFrance
MAIRIE DE PARIS

# Contexte

Il existe différents modèles de *libre accès*.

# Contexte

Il existe différents modèles de *libre accès*.

- *Voie verte* :
  - mise en ligne des articles directement par les chercheu·r/se·s,
  - utilisation de dépôts pérennes (archives nationales ou institutionnelles),
  - parallèle au circuit de publication traditionnel.

# Contexte

Il existe différents modèles de *libre accès*.

- *Voie verte* :
  - mise en ligne des articles directement par les chercheu·r/se·s,
  - utilisation de dépôts pérennes (archives nationales ou institutionnelles),
  - parallèle au circuit de publication traditionnel.
- *Voie dorée* :
  - accès libre directement depuis le site du *publisher*,
  - malheureusement détournée par leurs lobbies,
  - aujourd'hui $\approx$ auteur-payeur.

# Contexte

Il existe différents modèles de *libre accès*.

- *Voie verte* :
  - mise en ligne des articles directement par les chercheu·r/se·s,
  - utilisation de dépôts pérennes (archives nationales ou institutionnelles),
  - parallèle au circuit de publication traditionnel.
- *Voie dorée* :
  - accès libre directement depuis le site du *publisher*,
  - malheureusement détournée par leurs lobbies,
  - aujourd'hui $\approx$ auteur-payeur.
- *Voie diamant* :
  - faire des résultats de la recherche un *commun*,
  - reprise du contrôle par les chercheu·r/se·s de leurs moyens de production,
  - implique (entre autres) l'utilisation de logiciels libres à tous les niveaux.

# Contexte

Il existe différents modèles de *libre accès*.

- *Voie verte* :
  - mise en ligne des articles directement par les chercheu·r/se·s,
  - utilisation de dépôts pérennes (archives nationales ou institutionnelles),
  - parallèle au circuit de publication traditionnel.
- *Voie dorée* :
  - accès libre directement depuis le site du *publisher*,
  - malheureusement détournée par leurs lobbies,
  - aujourd'hui $\approx$ auteur-payeur.
- *Voie diamant* :
  - faire des résultats de la recherche un *commun*,
  - reprise du contrôle par les chercheu·r/se·s de leurs moyens de production,
  - implique (entre autres) l'utilisation de logiciels libres à tous les niveaux.

$\Rightarrow$ Nous avons besoin de l'aide de la communauté du libre !

# Stratégie

Nous sommes en période de transition.

- La question est : vers quel modèle ?
- Le dépôt en archives pérennes :

# Stratégie

Nous sommes en période de transition.

- La question est : vers quel modèle ?
- Le dépôt en archives pérennes :
  - encourage la prise de conscience des chercheu·r/se·s ;

# Stratégie

Nous sommes en période de transition.

- La question est : vers quel modèle ?
- Le dépôt en archives pérennes :
  - encourage la prise de conscience des chercheu·r/se·s ;
  - permet l'accès à tou·te·s aux articles déposés (y compris ceux déjà publiés) ;

# Stratégie

Nous sommes en période de transition.

- La question est : vers quel modèle ?
- Le dépôt en archives pérennes :
  - encourage la prise de conscience des chercheu·r/se·s ;
  - permet l'accès à tou·te·s aux articles déposés (y compris ceux déjà publiés) ;
  - sert de socle pour la transition vers le modèle de la voie diamant qui l'utilise.

# Stratégie

Nous sommes en période de transition.

- La question est : vers quel modèle ?
- Le dépôt en archives pérennes :
  - encourage la prise de conscience des chercheu·r/se·s ;
  - permet l'accès à tou·te·s aux articles déposés (y compris ceux déjà publiés) ;
  - sert de socle pour la transition vers le modèle de la voie diamant qui l'utilise.
- Obstacles au dépôt :
  - méconnaissances de leurs droits par les chercheu·r/se·s,
  - complexité de l'opération de dépôt dans certaines archives (coucou HAL).

# Stratégie

Nous sommes en période de transition.

- La question est : vers quel modèle ?
- Le dépôt en archives pérennes :
  - encourage la prise de conscience des chercheu·r/se·s ;
  - permet l'accès à tou·te·s aux articles déposés (y compris ceux déjà publiés) ;
  - sert de socle pour la transition vers le modèle de la voie diamant qui l'utilise.
- Obstacles au dépôt :
  - méconnaissances de leurs droits par les chercheu·r/se·s,
  - complexité de l'opération de dépôt dans certaines archives (coucou HAL).

$\Rightarrow$ Le but de Dissemin est d'optimiser le nombre de dépôts en archives pérennes.

# Dissemin

Dissemin est une plateforme libre qui simplifie le dépôt en archives pérennes.

- Pour chaque chercheu·r/se, Dissemin :
  - affiche une liste de ses publications ;
  - informe sur le taux de publications :
    - disponibles en libre accès,
    - qui pourraient être disponibles en libre accès mais ne le sont pas,
    - dont on ne connaît pas le statut,
    - dont le *publisher* interdit la mise en ligne.
- Pour chaque publication, Dissemin :
  - récupère les méta-données,
  - propose un accès direct au PDF si il en existe une version accessible,
  - propose d'en faire le **dépôt en un clic** dans une archive pérenne.

# Démonstration

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:*

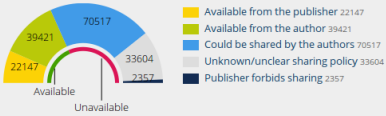
Firstname Lastname Search

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.

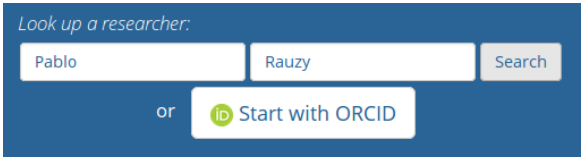
This forces libraries to buy overpriced electronic subscriptions to journals, when they can afford them at all.

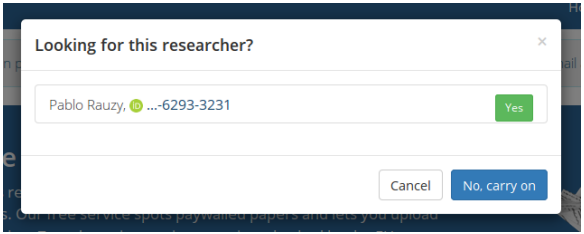



## Open repositories

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

Agnes Kiss, Juliane Krämer, **Pablo Rauzy**, Jean-Pierre Seifert — 2016

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

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

**Pablo Rauzy**, Sylvain Guilley, Zakaria Najm — 2015

### 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).

**Pablo Rauzy**, Sylvain Guilley — 2014

### 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 BellCoRe Attack: A Pledge for Formal Methods in the Field of

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

# 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

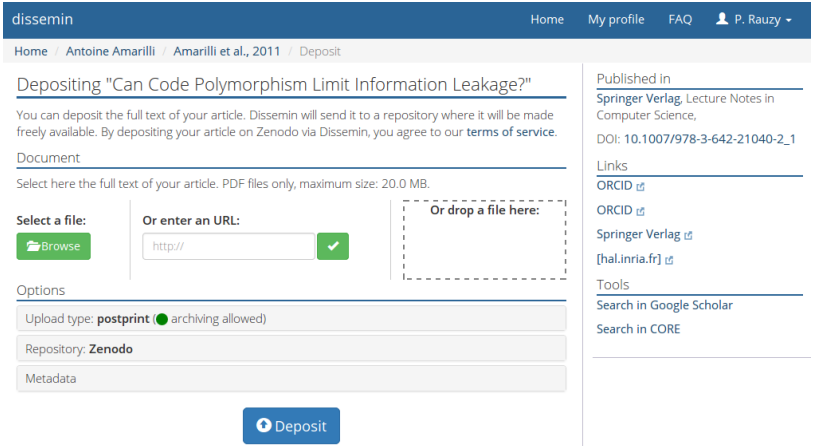
Springer Verlag

[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

# Développement

Dissemin est un logiciel libre.

- Code :
  - `https://github.com/dissemin`,
  - Principalement du Python (+ HTML, CSS, JavaScript).
- Équipe :
  - une dizaine de personnes gravitent autour du projet (conseils, aide ponctuelle, discussions),
  - les efforts de développement sont principalement portés par Antonin Delpeuch (pintoch),

  $\Rightarrow$ des mains (et cerveaux) supplémentaires feraient du bien !
- Sources des données :
  - Primaires :
    - CrossRef.org,
    - BASE,
    - SHERPA/RoMEO,
    - Zotero.
  - Secondaires (via OAI-PMH) :
    - arXiv, HAL, PubMed Central, OpenAIRE, DOAJ, Persée, Cairn.info, Numdam.

# DOAI

À chaque publication scientifique est assigné un DOI.

- DOI signifie "*Digital Object Identifier*".
- C'est très pratique...
- Mais c'est contrôlé ($\pm$ directement) par les *publishers*.
- Du coup un DOI pointe vers le $mur\ à\ péage$ du *publisher*.
- DOAI est un $résolveur\ alternatif$ qui pointe directement vers une version en libre accès, quand c'est possible.
- Il suffit pour cela de remplacer `http://dx.doi.org/` par `http://doai.io/` dans les liens :

`http://dx.doi.org/10.1007/s13389-015-0105-2`

↓

`http://doai.io/10.1007/s13389-015-0105-2`

# OAbot

Le libre accès permet d'améliorer Wikipédia.

- Autant que possible, les sources des articles Wikipédia sont citées.
- Souvent ces sources sont des articles de recherche.
- OAbot remplace automatiquement les liens vers des murs à péages par des liens vers une version en libre accès quand c'est possible.
- OAbot utilise CrossRef, BASE, et DOAI.

⇒ Toute aide est la bienvenue : `https://en.wikipedia.org/wiki/Wikipedia:OABOT`.

# Merci

Highlights :

- Les résultats de la recherche devraient être un *commun de la connaissance* pour profiter à tou·te·s.
- La transition vers le libre accès ouvre la voie vers cet objectif.
- Le modèle “diamant” permettrait de l’atteindre.
- Ce modèle nécessite des infrastructures libres, notamment logicielles.

$\Rightarrow$ On a besoin de vous !

Questions ?