

Les communs, le libre accès, et Dissemin

Pablo Rauzy

`pablo.rauzy@univ-paris8.fr`

`https://pablo.rauzy.name/`



Journée OpenAIRE

27 juin 2017



WIKIPEDIA



WIKIP€DIA



WIKIP€DIA

- ▶ Tou·te·s peuvent rédiger des articles.
- ▶ Tou·te·s peuvent les corriger.



WIKIP€DIA

- ▶ Tou·te·s peuvent rédiger des articles.
- ▶ Tou·te·s peuvent les corriger.
- ▶ Seulement 30€ pour consulter un article !



- ▶ Tou·te·s peuvent rédiger des articles.
- ▶ Tou·te·s peuvent les corriger.
- ▶ Seulement 30€ pour consulter un article !
- ▶ Abonnements annuels :

PERSONNEL	1000 €	3 articles / jour
PERSONNEL	5000 €	accès illimité !
INSTITUTION	50 000 €	5 articles / jour / pers.
INSTITUTION	300 000 €	accès illimité !



1. La recherche d'une question.
2. La recherche d'une réponse.
3. L'obtention de résultats.
4. La rédaction d'un article.
5. La soumission de l'article.
6. L'évaluation par les pairs.
7. La publication de l'article.

preprint

postprint

version publiée

- ▶ La mise en page des articles.
- ▶ Distribuer le plus largement possible les articles.
- ▶ Gagner de l'argent.
- ▶ Faire (re)connaître les chercheurs.

- ▶ L'argent public finance la recherche :
 - personnes, locaux, matériel, etc.,
 - le contrôle de la qualité,
 - et parfois même sa publication.

- ▶ L'argent public finance la recherche :
 - personnes, locaux, matériel, etc.,
 - le contrôle de la qualité,
 - et parfois même sa publication.

- ▶ Puis les maisons d'éditions exigent une cessation de copyright :
 - appropriation privée des produits de la recherche
 - revendus au public (universités et laboratoires)
 - à des prix exorbitants.

Service commun de documentation (SCD) :

- ▶ Montant total des dépenses : 2 101 587,47 €
- ▶ Dont dépenses documentaires : 1 083 885,16 €

Service commun de documentation (SCD) :

- ▶ Montant total des dépenses : 2 101 587,47 €
- ▶ Dont dépenses documentaires : 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. »

Coût : exemple du CNRS (2013)

- Dépenses documentaires : ~36 millions d'€.

Bénéfices : exemple de Reed-Elsevier (2013)

- ▶ Revenus : ~ 7 milliards d'€ (+3%).
- ▶ Bénéfices : 2+ milliards d'€ (+5%).

- ▶ Le coût en € est un symptôme, pas le problème réel.
- ▶ Accès citoyen.
- ▶ Égalité entre étudiant·e·s, chercheuses et chercheurs.
- ▶ Entre universités et dans le monde entier.

« La mise à disposition des publications et des données de la recherche en accès libre, gratuit et illimité sur **Internet**, sans restriction de paiement ou d'abonnement pris auprès d'éditeurs ou de sociétés savantes. »

Il existe différents modèles de *libre accès*.

Il existe différents modèles de *libre accès*.

► *Voie verte* :

- mise en ligne des articles directement par les chercheur·e·s,
- utilisation de dépôts pérennes (archives nationales ou institutionnelles),
- parallèle au circuit de publication traditionnel.

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.

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.

Nous sommes en période de transition.

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

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 ;

Nous sommes en période de transition.

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

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.

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.

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.
- ⇒ Le but de Dissemin est d'optimiser le nombre de dépôts en archives pérennes.

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

► Pour chaque chercheur·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.

`http://dissem.in/`

dissemin.in is currently in public beta. Please, let us know about any issue you might have, either on [Github](#) or by email at bugs@dissemin.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:

or



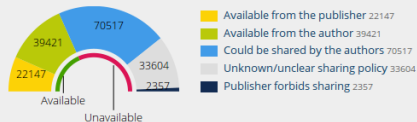
Start with ORCID



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.

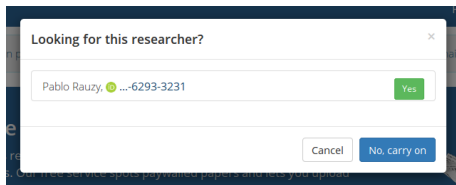
Dissemin searches for copies of your papers in a large collection of open repositories and tells you which ones cannot be accessed.

Look up a researcher:

Pablo	Rauzy	Search
-------	-------	--------

or

 Start with ORCID



Papers authored by Pablo Rauzy



Agnes 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, .

2016



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).

2015



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

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

[Download](#) | 2014 Workshop on Fault Diagnosis and Tolerance in Cryptography.

2014



Pablo Rauzy, Sylvain Guilley

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

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 F_i before its execution. The outcome is a genealogy of programs $F_0, F_1, \dots$ such that for all inputs x and for all indexes $i \neq j \Rightarrow F_i(x) \neq F_j(x)$ and $F_i \neq F_j$. 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

HomeMy profileFAQP. 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:


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 

Repository:



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 F_i before its execution. The outcome is a genealogy of programs $F_0, F_1, \dots$ such that for all inputs x and for all indexes $i \neq j \Rightarrow F_i(x) \neq F_j(x)$ and $F_i \neq F_j$. 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

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



HAL is a multidisciplinary open archive, sustained by the French Research Ministry.

Metadata

Abstract*

This work revisits set reconciliation, the problem of synchronizing two multisets of fixed-size values while minimizing transmission complexity. We propose a new number-theoretic reconciliation protocol called Divide and Factor (D&F) that achieves optimal asymptotic transmission complexity – as do previously known alternative algorithms. We analyze the computational complexities of various D&F variants, study the problem of synchronizing sets of variable-size files using hash functions and apply D&F to synchronize file hierarchies taking file locations into account. We describe btrsync, our open-source D&F implementation, and benchmark it against the popular software rsync. It appears that btrsync transmits much less data than rsync, at the expense of a relatively modest computational overhead.

Scientific field*

Computer science

Depositing author*

Pablo Rauzy

Affiliation*

My deposits

"Algorithmic Countermeasures Against Fault Attacks and Power Analysis for RSA-CRT" in HAL	
Paper	Algorithmic Countermeasures Against Fault Attacks and Power Analysis for RSA-CRT
Repository	HAL
Deposit date	Feb. 7, 2017, 10:51 p.m.
Deposit type	Postprint
Identifier	hal-01461208
Meta URL	https://hal.archives-ouvertes.fr/hal-01461208
PDF URL	https://hal.archives-ouvertes.fr/hal-01461208/document
Status	Published
Password	

Preferences

General

HAL

Email

We will use this email address to notify you when your deposits are accepted.

Preferred repository

- ☐ No preferred repository
- ☒ Zenodo
- ☐ HAL

This repository will be used by default for your deposits.

Save

Preferences

General

HAL

HAL username

p4bl0

If set, deposits will be associated to this HAL account.

Save

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 Delpuech (pintoeh),
- ⇒ 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.



Atelier

Hackathon Plateforme Dissem.in

Atelier de développement du code et de dépôt d'articles de recherche dans HAL ou Zenodo via <http://dissem.in>

Participants : Chercheurs et développeurs

Samedi 8 juillet 2017, 10h-20h,

salle de Conf IV, 2ième étage, Département de Physique
ENS, 24 rue Lhomond Paris 5ième

Organisateurs : PSL et CAPSH
Contact : Marie Farge / marie.farge@gmail.com
Programme détaillé : www.ens.fr (rubrique agenda)

École normale supérieure,
45 rue d'Ulm, 75005 Paris



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`

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>.

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.

Questions ?