

Checkresearch.org

User Manual 0.8

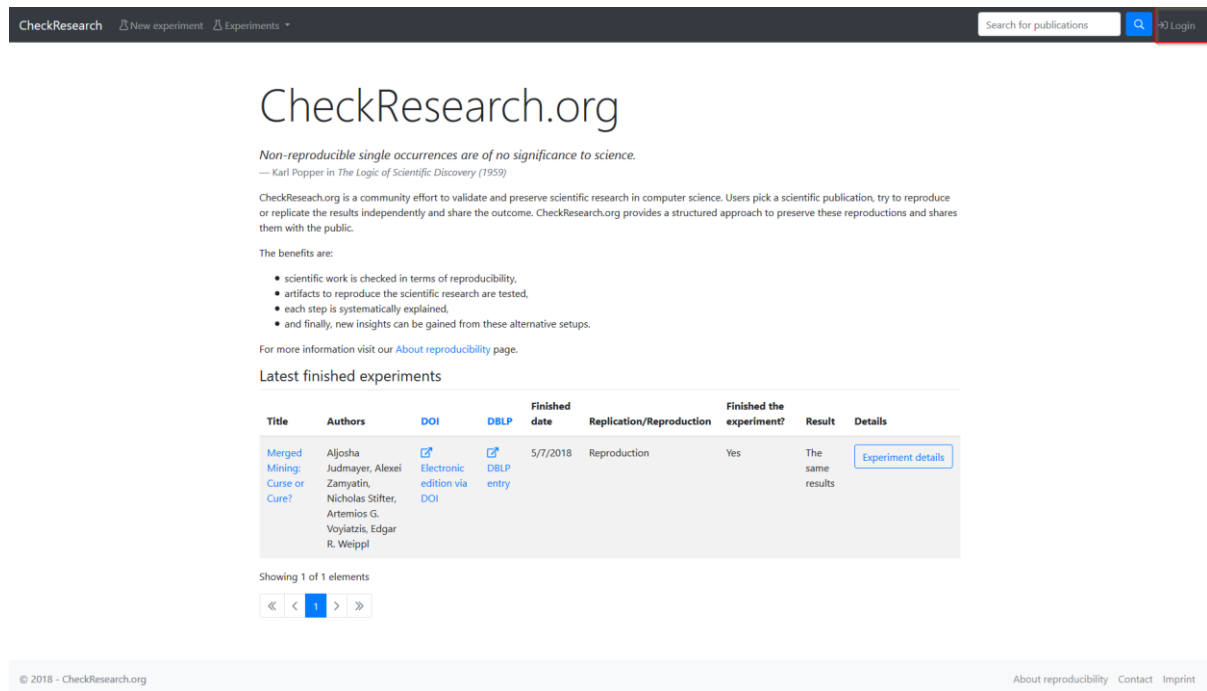
Table of Contents

1	Editor.....	2
1.1	Register.....	2
1.2	Create a new Experiment.....	5
1.2.1	GitHub Repository and Directory Structure	9
1.3	Re-opening of Experiments	11

1 Editor

1.1 Register

Visit: www.checkresearch.org, click on "Log in" in the upper right corner.



CheckResearch.org

Non-reproducible single occurrences are of no significance to science.
— Karl Popper in *The Logic of Scientific Discovery* (1959)

CheckResearch.org is a community effort to validate and preserve scientific research in computer science. Users pick a scientific publication, try to reproduce or replicate the results independently and share the outcome. CheckResearch.org provides a structured approach to preserve these reproductions and shares them with the public.

The benefits are:

- scientific work is checked in terms of reproducibility,
- artifacts to reproduce the scientific research are tested,
- each step is systematically explained,
- and finally, new insights can be gained from these alternative setups.

For more information visit our [About reproducibility](#) page.

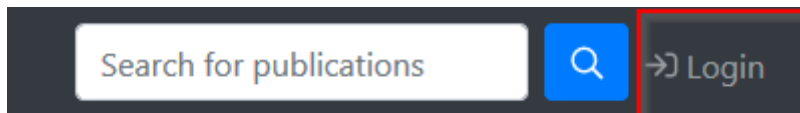
Latest finished experiments


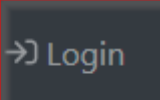
Title	Authors	DOI	DBLP	Finished date	Replication/Reproduction	Finished the experiment?	Result	Details
Merged Mining: Curse or Cure?	Aljosa Judmayer, Alexei Zamiatin, Nicholas Stifter, Artemios G. Voyiatzis, Edgar R. Weippal	Electronic edition via DOI	DBLP entry	5/7/2018	Reproduction	Yes	The same results	Experiment details

Showing 1 of 1 elements

« < 1 > »

© 2018 - CheckResearch.org [About reproducibility](#) [Contact](#) [Imprint](#)



Search for publications  

Log in

Use a local account to log in.

Username or Email

Password

Remember me?

Log in

[Forgot your password?](#)

[Register as a new user?](#)

Use another service to log in.

 GitHub

 Google

To get access to the platform, you can either register directly or log in using your existing Google- or GitHub account. If you choose to register directly, you will see the following mask:

Register

Create a new account.

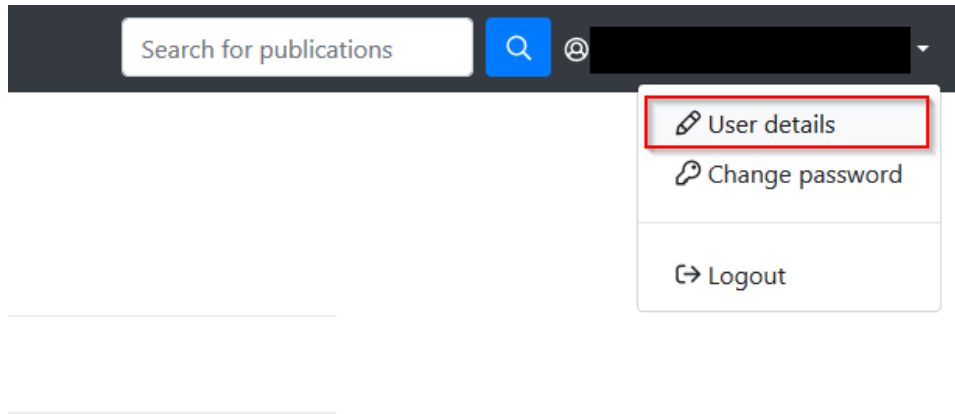
Email

Password

Confirm password

Register

Type in your email address and the password you wish. It does have to contain at least one digit, however. Once you are logged in, you can click at the right upper corner again, then on "User details".



Here you can add additional ways to log in if wished.

Manage your account

Change your account settings

[Profile](#) [Add another service to log in.](#)

[Password](#)

[External logins](#) [GitHub](#) [Google](#)

[Two-factor authentication](#)

1.2 Create a new Experiment

In the upper left corner, click on "New experiment".



CheckResearch.org

Before you create a new experiment, you should search if there already exists a reproduction of the publication you want to reproduce.

Advanced search (conjunctive)

Publication title

Name of author or editor

Title of journal or proceeding

Year of publication

Search results

Title	Authors	DOI	Year	Publication type	Details	New experiment
The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli.	Matúš Nemeč, Marek Šýs, Petr Svenda, Dusan Klíneč, Vashek Matyas	10.1145/3133956.3133969	2017	InProceedings	<input type="button" value="View"/>	<input type="button" value="Choose"/>

If not, click on "Import publication" in order to create a new experiment with reference to a publication via DOI or DBLP key.

Advanced search (conjunctive)

Publication title

Name of author or editor

Title of journal or proceeding

Year of publication

Lookup Publication

Fetch publication data from DBLP by entering the DBLP-Key or the DOI.

Key

Use the [DBLP search](#) to find the key.

Doi

An output similar to this one indicates the successful import. No further steps have to be performed. Just click on "choose".

Found entry in DBLP: conf/ccs/NemecSSKM17

Publication "The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli." successfully created

Search results

Title	Authors	DOI	Year	Publication type	Details	New experiment
The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli	Matús Nemec, Marek Šýs, Petr Svenda, Dusan Klinec, Vashek Matyas		2017	Article	<input type="button" value="View"/>	<input checked="" type="button" value="Choose"/>

Showing 1 of 1 elements

« < 1 > »

If (and only if) neither DOI nor DBLP key exists for your publication, click on "Create publication".

Advanced search (conjunctive)

Publication title

Name of author or editor

Title of journal or proceeding

Year of publication

Before you create a new experiment, you have the option to search if a similar experiment already exists. For creating a new one, click on "+Create publication". Then fill out the form.

Refer to your paper either by DBLP reference or via DOI.

Create new Publication

Key

Doi

Title

Year

Person

Person

Person

Person

Person

Type

You need to copy the dblp key (E.g., *conf/ccs/NemecSSKM17*) or the DOI of the paper you want. Then click "create". You will now see your newly published experiment at the bottom at the "Search results". Click on "choose" in order to start working with it.

Search results

Title	Authors	DOI	Year	Publication type	Details	New experiment
The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli	Matús Nemec, Marek Sys, Petr Svenda, Dusan Klinec, Vashek Matyas		2017	Article	View	✓ Choose

Showing 1 of 1 elements

Create new Experiment

Publication

Publication title	The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli
Publication authors	Matús Nemeč, Marek Šys, Petr Svenda, Dusan Klinec, Vashek Matyas
DOI	
Year	2017
Publication Type	Article

Publication artifact links

Advisor's username or email (optional)

e.g.: advisor@example.com

GitHub user

GitHub repository name

confccsNemečSSKM17_Experiment_01

GitHub repository description

Repository for the reproduction of the work in "The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli" by "Matús Nemeč, Ma

GitHub project url

<https://checkresearch.org/Experiment/View/fae3f9e6-69bc-46d2-8cb3-97440a6874be>

+ Create

Enter your preferred GitHub user. Then copy and checkout the GitHub Project Url in order to push code, data, etc. When done, click on "create".

Experiment by "bbrenner@sba-research.org" for "conf/ccs/NemečSSKM17"

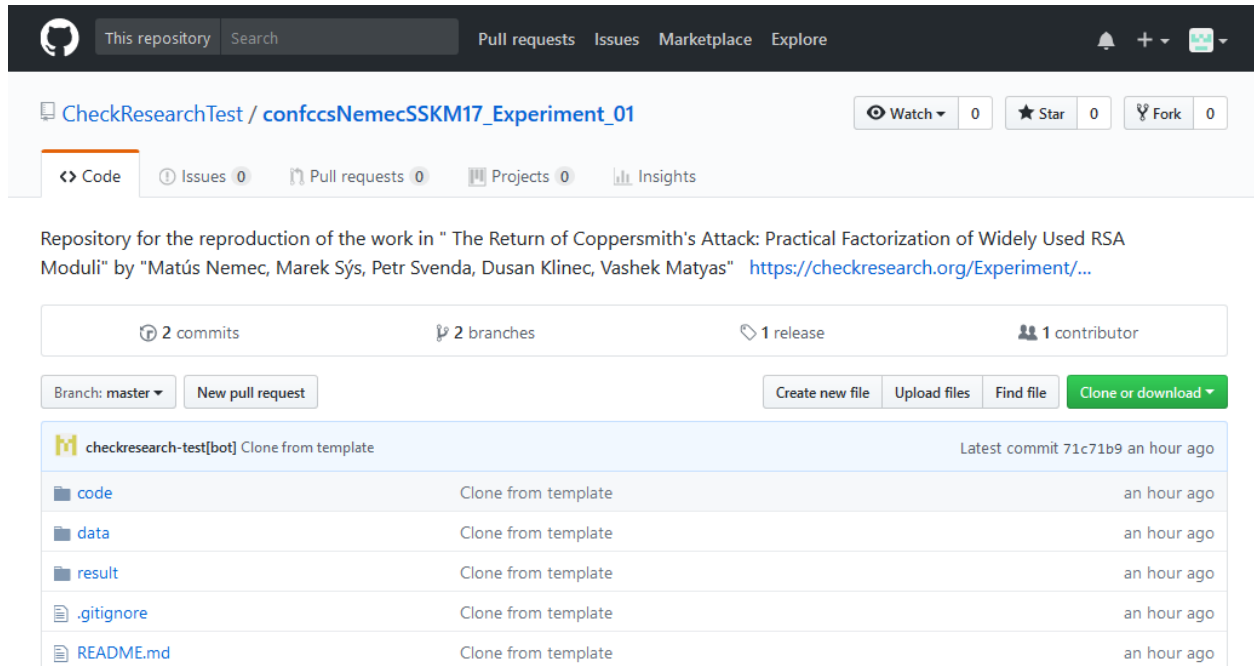
GitHub	Please wait while the GitHub repository is being created. Page reloads automatically!
Assigned user	bbrenner@sba-research.org
Start date	5/7/2018
Title	The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli
Authors	Matús Nemeč, Marek Šys, Petr Svenda, Dusan Klinec, Vashek Matyas
DBLP entry	DBLP entry
Status	In progress

✓ Finish experiment

🗑 Delete experiment

You should then see a page like this one. Please push all your code, etc to this repository. You may return to this page at a later time.

1.2.1 GitHub Repository and Directory Structure



The screenshot shows a GitHub repository page. At the top, there's a navigation bar with 'This repository', a search bar, and links for 'Pull requests', 'Issues', 'Marketplace', and 'Explore'. Below this, the repository name 'CheckResearchTest / confccsNemecSSKM17_Experiment_01' is displayed, along with 'Watch 0', 'Star 0', and 'Fork 0' buttons. A secondary navigation bar includes 'Code', 'Issues 0', 'Pull requests 0', 'Projects 0', and 'Insights'. The main content area features a description: 'Repository for the reproduction of the work in "The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli" by "Matús Nemeč, Marek Sýs, Petr Svenda, Dusan Klinec, Vashek Matyas" <https://checkresearch.org/Experiment/...>'. Below the description, statistics show '2 commits', '2 branches', '1 release', and '1 contributor'. Action buttons include 'Branch: master', 'New pull request', 'Create new file', 'Upload files', 'Find file', and 'Clone or download'. A table lists files and folders: 'code', 'data', 'result', '.gitignore', and 'README.md', each with a 'Clone from template' link and a timestamp of 'an hour ago'.

Note that in the repository, there is a template directory structure that is automatically created by checkresearch:

```
\---YourProjectRoot
|   README.md
|
+---code
|   \---originalcode
+---data
|   \---originaldata
\---result
```

Please keep this structure in order to enable others to get used to it.

A short explanation of this template:

- [README.md](#): Please fill out the simple form in the README.md file once you are done with your reproduction. It will help others to know what you have done and run your experiments themselves.
 - Code: source code you created
 - Code/originalcode: (unchanged) source code from the authors
 - Data: data you created
 - Data/originaldata: (unchanged) data from the authors
 - Result: Output, etc.

Experiment by "bbrenner@sba-research.org" for "conf/ccs/NemecSSKM17"

GitHub	Please wait while the GitHub repository is being created. Page reloads automatically!
Assigned user	bbrenner@sba-research.org
Start date	5/7/2018
Title	The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli
Authors	Matús Nemeč, Marek Sys, Petr Svenda, Dusan Klinec, Vashek Matyas
DBLP entry	DBLP entry
Status	In progress

[✓ Finish experiment](#) [🗑 Delete experiment](#)

Please push all your work to this repository and, once you are sure that it is complete, click on "Finish experiment". Once an experiment is "finished", it is not possible to change (i.e. push) anything anymore. **Nevertheless:** If you need to change something (e.g. to correct a mistake, etc.) you can re-open the experiment, implement the desired changes, and close it again.

When you click on "Finish experiment", a short questionnaire will appear. Please fill it out.

Finish Experiment for "conf/ccs/NemecSSKM17"

Short summary of your experiment:

Nemec et al. have shown that keys generated in cryptographic smartcards with Infineon chips are based on constructed primes (as opposed to randomly chosen primes). they have shown ways to check a key for the property of being constructed that way and to practically break such kevs. We will reproduce and test the fingerprinting, the construction of such weak kevs and a part of the attack.

The summary shouldn't consist of more than 50 words.

What is your connection to the authors of the original research?

I am one of the authors

I replicated/reproduced:

Parts of the research

My experiment is a:

Reproduction

The difference between reproduction and replication is described on our [About page](#).

Did the authors provide all artifacts necessary to reproduce/replicate the research?

No

Which artifacts are missing?

Instructions
Data
Source code/tools

Is special equipment required?

No

I was able to finish the experiment:

Yes

The results were:

The same results

Were the instructions clear?

Yes

Are there open questions?

Afterwards, click on "Finish experiment" again.

All experiments by "bbrenner@sba-research.org"

Title	Authors	DOI	DBLP	Begin	End	Status	GitHub	Details
The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli	Matus Nemec, Marek Slys, Petr Svenda, Dusan Klinec, Vashek Matyas		DBLP entry	5/7/2018	5/7/2018	Finished	GitHub repository	Experiment details

You will then see an overview with all your experiments. Your experiment will also be visible on the title page.

1.3 Re-opening of Experiments

Re-opening of an experiment may be necessary if you want to correct a mistake, etc.

To re-open an experiment, follow the following steps.

Latest finished experiments

Title	Authors	DOI	DBLP	Finished date	Replication/Reproduction	Finished the experiment?	Result	Details
The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli	Matús Nemeč, Marek Šýs, Petr Svenda, Dusan Klinec, Vashek Matyas		DBLP entry	5/7/2018	Reproduction	Yes	The same results	Experiment details
Merged Mining: Curse or Cure?	Aljosh Judmayer, Alexei Zamyatin, Nicholas Stifter, Artemios G. Voyiatzis, Edgar R. Weippl	Electronic edition via DOI	DBLP entry	5/7/2018	Reproduction	Yes	The same results	Experiment details

Showing 2 of 2 elements



In the list of experiments, click on the experiment you want to re-open (you must be one of the authors of the reproduction in order to be able to re-open it).

Click on "Open experiment again".

Experiment by "bbrenner@sba-research.org" for "conf/ccs/NemecSSKM17"

<p>GitHub</p> <p>Assigned user</p> <p>Start date</p> <p>Title</p> <p>Authors</p> <p>DBLP entry</p> <p>Status</p>	<p>GitHub repository</p> <p>bbrenner@sba-research.org</p> <p>5/7/2018</p> <p>The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli</p> <p>Matús Nemeč, Marek Šýs, Petr Svenda, Dusan Klinec, Vashek Matyas</p> <p>DBLP entry</p> <p>Finished</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Result from 5/7/2018 2:45 PM

Summary

Connection to the author

Extent

Type

Missing instructions

Missing data

Missing source

Experiment ended with

Instruction clarity

Duration of experiment

GitHub commit hash

[Open experiment again](#)

You can now push changes to the repository again. When done, click "Finish experiment" as before.