Isogeny-based cryptography
FWO DMP (Flemish Standard DMP)

1. Research Data Summary

List and describe all datasets or research materials that you plan to generate/collect or reuse during your research project. For each dataset or data type (observational, experimental etc.), provide a short name & description (sufficient for yourself to know what data it is about), indicate whether the data are newly generated/collected or reused, digital or physical, also indicate the type of the data (the kind of content), its technical format (file extension), and an estimate of the upper limit of the volume of the data.

				Only for digital data	Only for digital data	Only for digital data	Only for physical data
Dataset Name	Description	New or reused	Digital or Physical	Digital Data Type	Digital Data format	Digital data volume (MB/GB/TB)	Physical volume
		Please choose from the following options: • Generate new data • Reuse existing data	*Please choose from the following options:* • Digital • Physical	*Please choose from the following options:* • Observational • Experimental • Compiled/aggregated data • Simulation data • Software • Other • NA	*Please choose from the following options:* • .por, .xml, .tab, .csv,.pdf, .txt, .rtf, .dwg, .gml, … • NA	*Please choose from the following options:* • <100MB • <1GB • <100GB • <1TB • <5TB • <10TB • <50TB • >50TB • NA	
Code	Proof-of-concept implementations of new cryptogrpahic schemes and/or cryptanalytincal attacks developed during the project	Generate new data	Digital	Software	.txt, .sage, .m	<1GB	

If you reuse existing data, please specify the source, preferably by using a persistent identifier (e.g. DOI, Handle, URL etc.) per dataset or data type:

During the project existing software libraries may be reused, typically Sagemath or Magma scripts, in accordance with the licenses under which they are published.

Are there any ethical issues concerning the creation and/or use of the data (e.g. experiments on humans or animals, dual use)? Describe these issues in the comment section. Please refer to specific datasets or data types when appropriate.

- No

Will you process personal data? If so, briefly describe the kind of personal data you will use in the comment section. Please refer to specific datasets or data types when appropriate.

- No

Does your work have potential for commercial valorization (e.g. tech transfer, for example spin-offs, commercial exploitation, …)? If so, please comment per dataset or data type where appropriate.

- No

Do existing 3rd party agreements restrict exploitation or dissemination of the data you (re)use (e.g. Material/Data transfer agreements/ research collaboration agreements)? If so, please explain in the comment section to what data they relate and what restrictions are in place.

- No

Are there any other legal issues, such as intellectual property rights and ownership, to be managed related to the data you (re)use? If so, please explain in the comment section to what data they relate and which restrictions will be asserted.

- Yes

The software libraries that this code would use may be published under restrictive licenses. ANy software in this project that builds upon these libraries will therefore be also subject to licenses that take into account the restrictions of the licenses therein.

2. Documentation and Metadata

Clearly describe what approach will be followed to capture the accompanying information necessary to keep data understandable and usable, for yourself and others, now and in the future (e.g., in terms of documentation levels and types required, procedures used, Electronic Lab Notebooks, README.txt files, Codebook.tsv etc. where this information is recorded).

Any software code or script produced during this project will be documented in-file, according to the practices of the relevant language. Also, readme files will be included alongside, describing how to compile and/or operate the software and how to interpret the output produced.

Will a metadata standard be used to make it easier to find and reuse the data? If so, please specify (where appropriate per dataset or data type) which metadata standard will be used. If not, please specify (where appropriate per dataset or data type) which metadata will be created to make the data easier to find and reuse.

- No

Any software code made publicly available will be stored on the github.com website, which is an industry reference for open-source software, on the COSIC research group's github.com page (https://github.com/KULeuven-COSIC). It will be named according to the research publications that refer to it, and links to the source code's page will also be included in such publications.

3. Data storage & back-up during the research project

Where will the data be stored?

The publicly available software code and scripts will be primarily stored on the COSIC GitHub repository (https://github.com/KULeuven-COSIC). Code that is not publicly available will be stored on the COSIC research group's GitLab infrastructure, which is private and also maintained by the ICTS service of the ESAT department of the KU Leuven.

How will the data be backed up?

The publicly accessible COSIC GitHub repository (https://github.com/KULeuven-COSIC) is backed up automatically by GitHub. The COSIC research group's GitLab
infrastructure is maintained by the ICTS services of the ESAT department of the KU Leuven.

Is there currently sufficient storage & backup capacity during the project? If yes, specify concisely. If no or insufficient storage or backup capacities are available, then explain how this will be taken care of.

- Yes

How will you ensure that the data are securely stored and not accessed or modified by unauthorized persons?

During the course of the project, software code and scripts will be protected by access rights maintained by the ESAT network and within the GitLab.

What are the expected costs for data storage and backup during the research project? How will these costs be covered?

The costs of the GitLab maintenance are covered by the COSIC research group as part of the general IT costs. The use of GitHub is currently 5USD/month and is funded from general COSIC funds.

4. Data preservation after the end of the research project

Which data will be retained for at least five years (or longer, in agreement with other retention policies that are applicable) after the end of the project? In case some data cannot be preserved, clearly state the reasons for this (e.g. legal or contractual restrictions, storage/budget issues, institutional policies...).

All data will be preserved for 10 years according to KU Leuven RDM policy.

Where will these data be archived (stored and curated for the long-term)?

All data will be archived in several locations. First, the ESAT GitLab will hold the code and scripts so that it can be easily retrieved for further use by researchers; this data is backed up. Second, a copy of the totality of the data will be stored in the KU Leuven RDR.

What are the expected costs for data preservation during the expected retention period? How will these costs be covered?

Given the small size (< 1GB) of the data, the storage cost will either be free of charge, or already covered by COSIC's or KU

Leuven's IT costs.

5. Data sharing and reuse

Will the data (or part of the data) be made available for reuse after/during the project? In the comment section please explain per dataset or data type which data will be made available.

- Yes, in an Open Access repository
- Yes, in a restricted access repository (after approval, institutional access only, …)

Projects that are deemed advanced enough will be made publicly available on the COSIC's GitHub page, with appropriate licenses. All projects will be stored on COSIC's GitLab so that it can be shared (conditioned on internal approval) with other researchers.

If access is restricted, please specify who will be able to access the data and under what conditions.

For the projects stored internally on GitLab, approval will be granted to COSIC researchers, or affiliated, under the condition of legitimate use for further research. This acts as a sanity check so that the technology is not removed from COSIC's internal control without further approval.

Are there any factors that restrict or prevent the sharing of (some of) the data (e.g. as defined in an agreement with a 3rd party, legal restrictions)? Please explain in the comment section per dataset or data type where appropriate.

- No

Some open-source software libraries used during this project come with licenses that limit their commercial use, but no proprietary code will be used so that all projects can be made open-source without requiring further authorisation.

Where will the data be made available? If already known, please provide a repository per dataset or data type.

The data will be made publicly available on COSIC's GitHub account, as this is a widely-used repository for open-source code. Alternative access may be made
available via KU Leuven RDR.

When will the data be made available?

If software projects are in enough of a developed state, they will be made available upon publication of research results.

Which data usage licenses are you going to provide? If none, please explain why.

CC-BY 4.0 (data) and MIT license (code).
The data that is made publicly available will use appropriate licenses to permit the use of the code for further research, but prohibit commercial use, in addition to respecting any licenses of libraries used within.

Do you intend to add a PID/DOI/accession number to your dataset(s)? If already available, you have the option to provide it in the comment section.

- Yes

Yes, a PID will be added upon deposit in a data repository; the KU Leuven RDR will be used for this.

What are the expected costs for data sharing? How will these costs be covered?

Given the small size (< 1 GB), data sharing is expected to be free of charge.

6. Responsibilities

Who will manage data documentation and metadata during the research project?

The authors of the code are responsible.

Who will manage data storage and backup during the research project?

Daniel Ishimwe is the COSIC sysadmin in charge of linking the COSIC GitHub repository and internal GitLab repos with the KU Leuven RDR.

Who will manage data preservation and sharing?

Daniel Ishimwe is the COSIC sysadmin in charge of linking the COSIC GitHub repository and internal GitLab repos with the KU Leuven RDR.

Who will update and implement this DMP?

The PhD researcher following the project: Gioella Lorenzon.