INSTRUCTIONS FOR THE TECHNICAL ANNEX

**Instructions to prepare the Technical Annex**

**Use this template to prepare the Technical Annex of your proposal**. After completing all the chapters in this Word document, convert it to a single PDF document (maximum size 10MB) and upload it to the e-COST Submission Tool. **Please delete this instruction page** when saving the proposal to PDF and before uploading it to the e-COST Submission Tool.

Remember that the page limit of this Technical Annex constitutes one of the eligibility criteria, so make sure that its length **does not exceed 15 pages**. The template provided **must not be modified and the formatting be kept** (COST standard font style: Arial font, size 10, line spacing 1. To select this style, choose “Normal,Text” style option from the ribbon styles gallery).

When writing the Technical Annex **please closely follow the instructions in Section 3.4.2. TECHNICAL ANNEX** of the [COST Open Call Submission, Evaluation, Selection and Approval (SESA) Guidelines](http://www.cost.eu/proposal_sesa_guidelines), (pages 15-18); it is recommended to follow the writing style guide in Section 3.5 (page 19) of the same Guidelines..

**Disclaimer on Intellectual Property Rights and Copyright**: A proposal for a COST Action must respect fundamental ethical principles as described in the [COST Code of Conduct](https://www.cost.eu/wp-content/uploads/2018/10/COST-081-15-COST-Code-of-Conduct.pdf). COST strives to avoid the deliberate replication of ideas, data, results or other scientific work without due permission and acknowledgement. Make sure that the ideas developed in the proposal are yours (no plagiarism will be tolerated) and that you own, or have received the necessary authorisations from the intellectual property rights holders to validly use, all intellectual property rights on the photographs, slides, graphs, digital images or other material that you include in the Technical Annex.

**Special note on anonymity**: To be eligible, a proposal for a COST Action, in particular the Technical Annex, shall be **anonymous**, hence contain no **direct or indirect** reference to proposers and/or institutions participating in the network of proposers, meaning that proposers’ and/or institutions’ names should neither be explicitly mentioned nor be potentially identifiable. Please closely follow the [SESA Guidelines](http://www.cost.eu/proposal_sesa_guidelines) (p. 11-12, 16 and 18).

TECHNICAL ANNEX

# 1 S&T EXCELLENCE

Elliptic curves have been central to the development of number theory throughout the 20th century, and of public-key cryptography in the 21st century. Their interest and utility is beyond question. Contemporary **Elliptic Curve Cryptography (ECC)**, which is now ubiquitous in digital security (from the internet to smart cards), represents a brilliant example of effective exchange and collaboration between researchers from pure mathematics (especially number theory and algebraic geometry), computer science, and engineering. Now, the new emergence of **isogeny-based cryptography** requires us to strengthen, broaden, renew, and re-focus this exchange: this is the goal of the Action.

## 1.1 Soundness of the Challenge

**Elliptic curves** are simple cubic equations that are a valuable source of groups and representations in number theory. Since the landmark 1985 works of Koblitz and Miller, they have gradually become an indispensable tool for cryptographers. Elliptic-curve cryptosystems are now widely deployed, and represent the state-of-the-art for key establishment in secure internet connections, for digital signature schemes, and for authentication and encryption in smart cards.

**Isogenies** are algebraic mappings—essentially, nontrivial algebraic relationships—between elliptic curves. Isogenies play the elliptic-curve role that matrices play in linear algebra: for number theorists, they are fundamental to the study of elliptic curves. Until recently, isogenies have played a minor and somewhat hidden role in ECC: for example, they are crucial in the generation of secure ECC parameters (in the Schoof-Elkies-Atkin point counting algorithm), and they have also been used to map hard cryptographic problems between curves. However, it has been possible for researchers to learn and work in ECC without knowing about isogenies.

In the past decade, however, a new generation of public-key **isogeny-based cryptosystems** has appeared, rapidly gaining attention for their apparent resistance to adversaries equipped with quantum computers—a quality that classical ECC spectacularly lacks. Isogeny-based cryptography is the newest of the main paradigms in **post-quantum cryptography**, but it has already found some success: one early cryptosystem, SIKE, has been selected by the National Institute of Standards and Technology (NIST) as an alternate candidate in the third round of its post-quantum cryptography standardisation process.

In isogeny-based cryptosystems,

* *security* depends on the difficulty of reconstructing an unknown isogeny with classical and/or quantum computers;
* *utility* depends on highly efficient algorithms and software for computing isogenies; and
* proper *design and analysis* requires a deep understanding of the mathematical and algorithmic nature of isogenies.

From a cryptographic perspective, our understanding of these three aspects is still rudimentary and immature. The challenge now facing us is to renew, strengthen, and enlarge the collaboration between mathematicians, computer scientists, and engineers that was fundamental to the success of ECC, in order to better understand and establish the theory and practice of isogeny-based cryptography.

### 1.1.1 DESCRIPTION OF THE STATE-OF-THE-ART

The beginning of isogeny-based cryptography (as we recognise it today) goes back to 2006, with the early public-key cryptosystems sketched by Stolbunov and the isogeny-based hash function of Charles, Goren, and Lauter. The first competitive cryptosystem was Jao and De Feo’s SIDH (2009) post-quantum key exchange algorithm, which became the basis of the SIKE Key Encapsulation Mechanism (KEM) submitted to the NIST post-quantum standardisation process. Early research on isogeny-based cryptosystems was mostly focused on SIDH, its cryptanalysis, and its efficient implementation. As the most mature of isogeny-based cryptosystems, SIDH remains an important target.

In recent years, however, Stolbunov’s ideas have been revisited, producing an explosion of new cryptosystems based on the nexus of isogenies and class field theory. The most notable such cryptosystem is CSIDH, which promises to be the first post-quantum solution for non-interactive key exchange. The crucial idea is the realisation of cryptosystems based on *group actions*.

However, the mathematical foundations of Stolbunov’s cryptosystems and CSIDH lend themselves to more detailed constructions. We now have a new and efficient isogeny-based digital signature schemes, CSI-FiSh, and more advanced protocols such as threshold and ring signatures.

The flexibility of isogeny-based cryptosystems more generally has also recently come to light in, for example, another efficient isogeny-based digital signature scheme, SQISign, and isogeny-based Verifiable Delay Functions (VDF).

Conversely, these newer and more complicated cryptosystems require a more sophisticated security analysis, both classical and quantum. For example: SIDH security depends essentially on a claw-finding problem. Quantum claw-finding algorithms are relatively well-understood, and there is something of a consensus on their modelling and projected behaviour. In contrast, CSIDH security depends on an abelian hidden shift problem, which can be solved using Kuperberg’s quantum algorithm with a quantum isogeny-evaluation subroutine; but so far concrete estimates for the cost of these algorithms have been wildly divergent.

Going beyond specific cryptosystems, the development of isogeny-based cryptography requires a range of highly non-trivial supporting algorithms. For example: the CSI-FiSh signature scheme requires a massive precomputation of the ideal class group structure of a certain quadratic imaginary ring. Achieving this for the first proposed parameter set required a world-record class group computation by Beullens, Kleinjung, and Vercauteren. Instantiating schemes like CSI-FiSh at higher security levels, or with larger parameters in reaction to revised security estimates requires cutting-edge techniques in algebraic number theory, using algorithms that have been largely neglected by cryptographers for over a decade.

### 1.1.2 DESCRIPTION OF THE CHALLENGE (MAIN AIM)

To advance and deploy isogeny-based cryptosystems the Action requires

1. An effective, constructive, and algorithmic understanding of mathematical structures such as quaternion algebras which, while common in number theory, are poorly-known and understood among ECC researchers.
2. A better understanding of quantum algorithms, both established and new, and their application to fundamental problems with isogenies and more broadly in number theory.
3. The development and adaptation of tools and algorithms from algebraic number theory, such as class-group computations, that have not been used in ECC research before, and of which knowledge elsewhere in cryptography has grown stale.
4. More effective and open exchange and transmission of knowledge between researchers in cryptography and number theory, expanding an interdisciplinary bridge built by ECC.
5. Increased interaction between specialists in isogenies and theoretical cryptographers, with a view to defining new post-quantum protocols with solid foundations.
6. A determined and unified effort to demystify isogenies for working cryptographers and cryptographic engineers, rendering the field accessible to practitioners.

To do this, The action will put together a European research network of number theorists, cryptographers, and specialists in quantum algorithms. The network will be built upon a framework for fundamental research and effective communication, both within the network and with the broader international community.

## 1.2 Progress beyond the state-of-the-art

This Action can be reasonably expected to make significant progress beyond the state-of-the-art in three main topics: constructing new protocols, cryptanalysis, and implementation.

We see above that isogenies have proven already to be flexible in their breadth of cryptographic applications: (non-interactive) key exchange, signatures, VDFs, and more. However, many of the classical cryptographic protocols from later generations, for example using pairings, do not yet have efficient post-quantum analogues. The Action will have a focused Working Group on number-theoretic foundations in order to explore further the potential for new post-quantum as well as classical applications of isogenies; such a study may also lead to improved algorithms for the current popular isogeny-based constructions.

With cryptanalysis it is especially important that the best classical and quantum algorithms to attack isogeny-based cryptosystems are well understood and pushed to their limits, as well as searching for new approaches. By the end of the Action, we will have a unified stance on the classical and quantum security of SIKE and CSIDH, as well as more advanced protocols, and have a better understanding of the security of isogeny-based cryptography more generally. This will give much-needed confidence in the schemes before they are implemented on a wide-scale.

Secure and efficient implementation is a very active topic in isogeny-based cryptography. Through this Action, by the careful creation of databases and coordination of work it will be possible to present secure and optimised implementations for not only the main protocols but also for new constructions.

### 1.2.1 APPROACH TO THE CHALLENGE AND PROGRESS BEYOND THE STATE-OF-THE-ART

The Action approach to the challenge from the perspective of the network has two main foci: introducing young researchers to the main open problems while equipping them with the tools they will need, and bringing together researchers from different fields to learn from each others’ different perspectives.

Concretely, for the first aim a week-long Training School will be held near the beginning of the Action, and a book with chapters contributed by the lecturers of this school will be created. The book will be maintained on an open source online platform with possibility for the future addition (or removal) of chapters until the end of the Action, due to the fact that the topic is still changing rapidly, and will be formally published during the last year of the Action.

For the second aim, the Action will bring together researchers from different fields by means of both dedicate Working Groups and workshops, structured around the four pillars of number theoretic foundations, cryptanalysis, primitives and protocols, and implementations; as well as transversal activities involving more than one Working group.

Finally, the Action will support Short-Term Scientific Missions, especially to foster research connections formed at the aforementioned workshops, throughout the entire Action period. These missions will be vital for the continuation of the research inspired by the workshops, and especially prioritise mobility for young researchers and participants who do not have access to alternate travel funding.

### 1.2.2 Objectives

Although isogeny-based cryptography is still very much an emerging field, the time pressure of achieving post-quantum cryptographic standards and the resource benefits of using isogeny-based cryptosystems are facilitating the possibility of relatively early wide-scale adoption of isogeny-based cryptosystems. The objectives of the Action, listed below, aim to mitigate the risk of early adoption where possible as well as to develop a unified global outlook in the field. In particular, no one country involved in the Action (or indeed globally) has a critical mass of isogeny-based cryptography researchers; a research network will facilitate regular discourse and collaboration between both the European and international community.

#### 1.2.2.1 Research Coordination Objectives

1. Lead a global discussion to develop a common vocabulary across the various fields (cryptography, number theory, quantum computing), leading to a shared understanding of both classical and quantum algorithms used in isogeny-based cryptosystems.
2. Develop the field of isogeny-based cryptography both by improving the understanding of the existing protocols and by developing new protocols.
3. Facilitate access to foundational knowledge in isogeny-based cryptography, both for Early Career Investigators and newcomers to the field. This will include mathematical background, algorithms, and protocol design, and will be achieved for example through open access articles, books, blog posts, audiovisual media, and databases.
4. Provide input to international standardisation bodies such as NIST and ETSI. For example, by writing ‘Requests for Comment’ (RFCs), technical reports, and filing public comments for the NIST post-quantum competition.
5. Disseminate the work achieved through COST collaborations by presenting at high-profile international cryptography conferences.

#### 1.2.2.2 Capacity-building Objectives

1. Grow the field of isogeny-based cryptography by fostering existing research connections. Most of the innovative papers in the field have resulted from multinational collaborations facilitated by ad hoc workshops or visits; a research network will allow for much more regular collaboration and consequently give rise to a rapid increase in high-quality research output.
2. Foster interdisciplinary approaches by bringing together researchers from cryptography, number theory, and quantum computing, all of whom have different perspectives on the major open problems in isogeny-based cryptography.
3. Give collaboration opportunities and increased visibility to Early Career Investigators who would otherwise be isolated or limited to very few local collaborators by connecting them with the whole European isogeny-based cryptography community.
4. Promote diversity in the community, for example by ensuring a diverse consortium and by collaborating with Women in Numbers Europe.

# 2 NETWORKING EXCELLENCE

## 2.1 Added value of networking in S&T Excellence

Isogeny based cryptography is a relatively young field, which suffers from geographical dispersion and a small community size. On the other hand it has grown to a rich enough field that newcomers and the general public often lack accessible, complete and reliable information sources. On top of that, isogenies are often regarded as an exceptionally technical topic within the field of cryptography.

By developing and structuring an international interdisciplinar network of researchers interested in the topic, providing them with well organised technical knowledge, powerful tools, and collaboration venues, the Action will accelerate the development of isogeny based cryptography, improve understanding, lower entry barriers, and facilitate industry adoption.

### 2.1.1 Added value in relation to existing efforts at European and/or international level

The proposers are not aware of any international effort primarily targeting isogeny-based cryptography, present or past.

The yearly Elliptic Curve Cryptography (ECC) workshop (https://eccworkshop.org/) has often been the venue where researchers interested in isogeny based cryptography meet and start collaborations, and has also served as platform to form Early Career Investigators through the associated research school. However the share of isogeny based cryptography within the event stays somewhat limited, and can hardly reach all the public targeted by the Action.

Past European efforts related to the Action are:

* COST Action IC1306, Cryptography for Secure Digital Interaction, ended in 2018, bridging together several areas of cryptography.
* COST Action IC1403, CRYPTACUS (https://www.cryptacus.eu/), ended in 2018, focusing on the security of cryptographic hardware and software.
* The H2020 project PQcrypto (https://pqcrypto.eu.org/), ended in 2018, focusing on candidates to the NIST post-quantum competition.
* The Marie Skłodowska-Curie Innovative Training Network 643161, ECRYPT-NET (https://www.ecrypt.eu.org/), ended in 2019, developing advanced cryptographic techniques for the Internet of Things and the Cloud, including post-quantum solutions.
* The ALGANT network (http://algant.eu/), a training network targeting Masters and PhD in number theory, involving several European universities.

Currently running European efforts related to the Action are:

* ERC Grant 669891, Almacrypt (http://www.almacrypt.eu/), which mainly focuses on elliptic curve and integer factoring cryptanalyses, but has also occasionally touched upon isogeny based cryptography.
* ERC Grant 805031, EPOQUE, focusing on secure implementation of NIST post-quantum candidates.

The level of support these past and present project provide to isogeny based cryptography is very limited. By looking more broadly at public investments on research in cryptography, it is apparent that isogeny-based cryptography is underrepresented. By bringing to life a coordinated research effort on isogeny based cryptography, the Action will consolidate Europe’s lead on the topic, will bring it to a level of maturity otherwise hardly achievable, and will bootstrap a virtuous cycle leading to an increased representation of isogeny based cryptography in European and international research programmes.

## 2.2 ADDED VALUE OF NETWORKING IN IMPACT

Owing to its small community size, geographical dispersion, and high degree of interdisciplinarity, it has repeatedly been observed that the most impactful work in isogeny based cryptography is often the result of large international collaborations, gathering expertise from more than one field.

Research on isogeny based cryptography already happens through an international network, supported by various personal grants on a case by case basis. However this mode of functioning is exclusive, limiting participation to a small circle of insiders, holding innovation back, and potentially leading to stagnation in the field.

By facilitating exchanges, fostering new collaborations, lowering entry barriers, ensuring diversity, the Action will maximise impact of isogeny based cryptography, shaping the technological landscape in the near and long term.

### 2.2.1 SECURING THE CRITICAL MASS AND EXPERTISE

Europe already is a leader in isogeny based cryptography, with well established networks in Belgium, France, Germany, the Netherlands, Switzerland, and the UK. However, several isolated researchers work in other European and Near Neighbouring countries, with limited access to networks.

The Action brings together researchers from all these countries, securing the best experts in the field. The Training Schools and workshops will let many talented Early Career Researchers meet well established researchers in the field, fostering new collaborations, and accelerating the development of isogeny based cryptography by an order of magnitude.

The Action will pay a particular attention to helping underrepresented groups join in the research effort. To this end, it will seek the collaboration of the Women In Number Theory community (http://womeninnumbertheory.org/) and of the Centre International de Mathématiques Pures et Appliquées (https://www.cimpa.info/) for selected workshops.

### 2.2.2 INVOLVEMENT OF STAKEHOLDERS

The main outputs of the Action will be new cryptosystems and cryptanalyses, which will shape our technological future. The primary stakeholders in this effort are standardisation bodies, such as NIST or ETSI, and tech companies working in telecoms, cloud, IoT, etc. The Action will engage with standardisation bodies by publishing recommendations, whitepapers, requests for comments (RFC), and filing public comments; members of the Action will be encouraged to participate in standardisation panels when relevant.

Building on its already established ties with industry partners, the Action will reach to a broader audience in tech companies using a variety of dissemination channels: talks, technical blog posts, audio-visual media, open source code, etc. Co-locating workshops with major conferences that attract both an academic and an industrial audience will further increase impact for these stakeholders.

Finally, universities and other academic institutions offering graduate programs in cryptography, algebra, number theory and quantum algorithms will benefit from the educational material published by the Action, such as books and audio-visual content.

### 2.2.3 MUTUAL BENEFITS OF THE INVOLVEMENT OF SECONDARY PROPOSERS FROM NEAR NEIGHBOUR OR INTERNATIONAL PARTNER COUNTRIES OR INTERNATIONAL ORGANISATIONS

Beyond Europe, the countries with the strongest networks in isogeny based cryptography are Canada, and the United States. The involvement of these partners as secondary proposers is thus a natural step towards building a truly inclusive research network. The partnership will make it easier to disseminate the outputs of the Action to these international countries, and, reciprocally, it will help keep Action members informed on activities happening outside of Europe.

# 3 IMPACT

The aim of the Action is to expand the impact of isogenies on future communication technologies. By creating the conditions to adopt, safely and cost-effectively, isogeny-based protocols in future communication protocols, the Action will positively impact the competitiveness of Small and Mid-size Enterprises (SME) and large companies in Europe and beyond.

The Action will seek to maximise impact by disseminating results in written form (books, academic papers, whitepapers, blog posts), and by training a new generation of young researchers and engineers in the fundamental tools of isogeny-based cryptography.

## 3.1 IMPACT TO SCIENCE, SOCIETY AND COMPETITIVENESS, AND POTENTIAL FOR INNOVATION/BREAK-THROUGHS

### 3.1.1 SCIENTIFIC, TECHNOLOGICAL, AND/OR SOCIOECONOMIC IMPACTS (INCLUDING POTENTIAL INNOVATIONS AND/OR BREAKTHROUGHS)

NIST’s eventual standardisation of SIKE, possibly at some point within the time frame of the Action, or shortly thereafter, is the first clear impact factor tied to the Action. Through its published analyses, the Action will aim at influencing NIST’s decision process. Two outcomes are possible: either the analyses shed doubt on the security of SIKE, an unfortunate outcome, but a valuable contribution to NIST and to society; or they confirm the strength of SIKE, and possibly improve its performance, paving the way for widespread adoption as well as growth in the sector of post-quantum cryptography.

While the eventual standardisation of SIKE will be an undeniable booster for the popularity of isogeny-based cryptography, the Action goals reach beyond NIST’s competition and post-quantum cryptography alone.

Within the scope of post-quantum cryptography, the Action will explore many significant innovations, such as, for example, efficient isogeny-based signature schemes, new advanced primitives not currently known to be constructible from isogenies, better provable security for already known primitives, and more in-depth analyses of available attacks. Although on a longer time-scale than SIKE, these innovations will directly benefit stakeholders operating in the post-quantum space such as SMEs and large companies offering encrypted products with long-term security.

Beyond post-quantum cryptography, the recently discovered “time delay protocols” based on isogenies offer another opportunity for high impact, providing cost-effective solutions to difficult problems in distributed computing such as generation of fair randomness or electronic voting. The primary beneficiaries of these technologies are stakeholders working with blockchains, and more generally financial services. The Action will advance the state-of-the-art of time delay protocols, providing more powerful constructions, more efficient protocols, and more secure instantiations.

Finally, in terms of scientific impact, the goal of the Action is to establish a common language and to reach a critical mass capable of accelerating progress in isogeny-based cryptography. The various actions described in the implementation section (workshops, schools, books) will contribute to form a new generation of experts with a deep understanding of isogeny-based cryptography, whose impact in the broader field of cryptography —both theoretical and applied— will be felt well after the Action is over.

## 3.2 MEASURES TO MAXIMISE IMPACT

### 3.2.1 KNOWLEDGE CREATION, TRANSFER OF KNOWLEDGE AND CAREER DEVELOPMENT

Owing to its interdisciplinary nature, and to the wide range of skills involved, the Action will alternate large meetings aimed at all partners and smaller focused meetings gathering participants from one or two Working Groups.

Concretely, the Action will be structured around yearly meetings, in rotating locations, aimed at all participants and open to outside researchers. The meeting will have both an educational component, in the form of lectures, and a research one, in the form of contributed talks, posters, and work sessions. To encourage outside participation, the Action will seek to co-locate the meetings with related conferences, e.g., Eurocrypt or ANTS. Lecturers will be encouraged to write lecture notes, and the notes will be collected on the website of the Action. Whenever technically possible, measures will be taken to also encourage remote participation; at a minimum, lectures will be recorded and made available online shortly after the workshop.

Between yearly meetings, the Action will organise smaller workshops or schools focused on narrower topics, typically involving one or two Working Groups. The workshops will primarily be targeted at Action members, but will be open to anyone, within the capacity of the event. Whenever feasible, these workshops will be organised in participating Inclusiveness Target Countries, to facilitate participation of their researchers. The format of the workshop will be decided by the organisers, and will have to be validated by the Management Committee.

Both for meetings and workshops, the Action will strive to involve young researchers in their organisation, in particular from Inclusiveness Target Countries, to encourage responsibility taking and network building.

A limited amount of Short-Term Scientific Missions and Conference Grants will be reserved to encourage PhD students to visit other institutions and develop scientific collaborations.

### 3.2.2 PLAN FOR DISSEMINATION AND/OR EXPLOITATION AND DIALOGUE WITH THE GENERAL PUBLIC OR POLICY

Throughout the duration of the Action, the official website will serve as a one stop shop for all sorts of resources related to the Action. In particular, it will contain:

* News feeds, agenda, links to mailing lists and social media accounts providing information on the Action’s activities.
* A regularly updated blog (1 post per month on average at least) discussing scientific topics related to the Action using an informal style.
* A database of all scientific publications in the field of isogeny based cryptography, both by Action members and non-members, searchable and downloadable in machine readable formats.
* Lecture material from the Action’s meetings and workshops.
* Information on the management of the Action.

The website will be maintained for at least 4 years after the end of the Action. The aim is for it to become a standard source of information for the field, and be kept up to date in the long term.

In the last year of the Action, selected lectures from the Training Schools, plus invited essays if necessary, will be considered to become chapters of a book edited under the supervision of the Action and published with an academic publisher.

The Action will disseminate its scientific discoveries through the usual academic channels. Green or gold open access will be the preferred publication model; fortunately, this is often the standard model in the appropriate communities. Datasets published by the Action (e.g., tables of polynomials, formulas, …) will follow standard open data practices. The Action will generally not seek to establish patents, as these are typically considered a hindrance to the deployment of cryptosystems. Exceptions may be made when a member seeks to establish a “defensive patent”; in this case the member will be required to explicitly release the patent to the public domain royalty-free.

The Action will target strategic venues for its communications: major conferences and journals in cryptography and number theory, targeted workshops on post-quantum cryptography, and standardisation body meetings. In particular, the Action will target the workshops regularly organised by NIST as part of the post-quantum competition, by submitting whitepapers and contributed talks.

Software produced by the Action will mostly consist of research software for demonstrative purposes, or contributions to open source computer algebra systems (e.g., PARI/GP, Sagemath, Oscar, …). In both cases, the code will be published under standard open source licenses, such as the GPL. Occasionally, some of these software may be integrated in the products of the industrial partners of the Action. As a general rule, the open source license will still apply to the software; most companies in cryptography regularly work with open source software. If the open source license does cause a problem with an industrial partner however, the authors of the code may decide to grant an additional closed source license to the industrial partner.

Besides advancing the state-of-the-art, the Action also aims at making isogeny-based cryptography accessible to as wide an audience as possible. The blog will be the primary communication medium targeted at the general public, and shall thus be rich in expository informal articles and links to further reading. A series of short introductory videos targeting Masters and PhD students will be recorded to complement the lectures given at Training Schools.

# 4 IMPLEMENTATION

## 4.1 COHERENCE AND EFFECTIVENESS OF THE WORK PLAN

### 4.1.1 DESCRIPTION OF WORKING GROUPS, TASKS AND ACTIVITIES

Due to its multidisciplinary nature, the Action brings together several communities with different expertise and vocabularies. The work plan will be structured around 4 Working Groups (WG), roughly corresponding to each of the communities, as described below.

**WG1 - Number theoretic foundations** This WG will be concerned with the mathematical foundations of isogeny-based cryptography, rooted in number theory and algebraic geometry. It will study the objects upon which cryptographic protocols are built, their generalisations and their algorithmic properties. In particular, it will research efficient algorithms for working with isogenies of elliptic curves and higher dimensional abelian varieties, the structure of isogeny graphs, and the algorithmic relationships with their endomorphism rings. Its outputs will inform the other working groups on the best algorithmic ways to reach their goals, and on the potential risks to security. From the other WG, it will draw inspiration for useful properties to look for in the algebraic objects.

**WG2 - Cryptanalysis** This WG will focus on algorithms to break the concrete schemes that have been proposed. It shares with WG1 an interest for algorithms to navigate isogeny graphs, however it approaches them from a cryptographic perspective, focusing on the security definitions and the minor details that make each system unique. Unlike other WGs, it will have a strong focus on quantum algorithms. Security reductions will also be an object of study of this WG, in collaboration with WG3. Its outputs will be used to set parameters for different security levels, in coordination with WG4.

**WG3 - Primitives, Protocols and Assumptions** This WG will research new primitives and protocols that can be built from isogenies. It will monitor the emergence of new primitives that have a potential to be built from isogenies, and inform other WGs in the hope of coming with a working proposal. It will construct new protocols (mostly advanced ones that go beyond encryption and signatures) using the available primitives, and seek to make them as efficient as possible in collaboration with WG4. Inspired by protocols in other subfields (e.g., lattice based cryptography), it will propose new isogeny-based assumptions upon which new protocols can be constructed, and assess their security in collaboration with WG1 and WG2.

**WG4 - Hardware & Software implementations** This WG will produce high efficiency secure implementations of isogeny algorithms and protocols, both in hardware and in software. It will discuss with WG2 to determine the most efficient parameters for a given security level. It will interact with WG1 to seek new theoretically efficient algorithms for isogeny computations, that translate into fast software and hardware. The security of the implementations will be considered on both a software level, informed partly by WG2, and on a hardware level, taking for example side-channel and fault attacks into account. Additionally, theoretical hardware attacks and the theoretical security levels as computed by work in WG2 will be verified and refined by implementation and practical experiments with the attacks.

[We need to say something about transversality, risk management, and how we make the WG talk to each other]

### 4.1.2 DESCRIPTION OF DELIVERABLES AND TIMEFRAME

**D1, Month 3. Initial press release.** This press release will give an overview of the Action, focusing on the goals and impact, and show readers where to find more about the Action.

**D2, Month 3. Virtual events tools and guidelines.** In order to help organise virtual and hybrid events, to maximise participation of individuals with travel or budget constraints, and to foster continuous engagement of participants before and after the events, this Deliverable will propose a series of guidelines and recommended tools, to the attention of Action Members. Some of the recommended tools (e.g., chat servers, video conferencing rooms, virtual research environments) may be adopted as global solutions for the whole duration of the Action, not tied to a specific event.

**D3, Months 6-48. Website.** Create a website as a coherent reference on isogenies for researchers and a basis for training students and researchers new to the field. It will be first put together after an introductory workshop, and then maintained online and open source in order to allow for changes and additions. This resource will be informed by all four work packages in an ongoing manner.

**D4.1, Month 9. Security whitepaper on isogeny-based protocols.** This deliverable will summarise the state of knowledge on the security of isogeny-based protocols at the start of the Action and will serve as a starting point of WG2 and parts of WG3. It will start with a presentation of all cryptographic assumptions proposed in the area and how they relate to each other. Then it will describe existing classical and quantum algorithms to solve these problems and the concrete impact of these algorithms on protocols. It will conclude with recommendations for practitioners (i.e. how to choose parameters in an implementation), protocol designers (which assumptions to use) and cryptanalysts (interesting open problems to address).

**D4.2, Month 45. Updated security whitepaper on isogeny-based protocols.** This deliverable will update the security whitepaper produced in D3.1 at the end of the Action, informed especially by the research of WG2 and WG3. It will focus on new or improved attacks on isogeny-based cryptosystems and on new or clarified security assumptions that appear during the course of the Action as part of WG2 and WG3 respectively. It will again conclude with recommendations for practitioners, protocol designers, and cryptanalysts.

**D5, Month 24. Isogeny Formulas Database.** Create an online database with the formulas needed for isogeny computations and isogeny-based cryptography. These include classic formulas, such as Vélu’s, as well as more recent work, such as VeluSQRT, radical isogenies, and the new input from WP4. The final result will be a useful tool for both implementers and protocol designers: a comprehensive and easy-to-access overview of the literature with regards to isogeny computation formulas.

**D6, Month 42. Book on isogeny-based cryptography.** This textbook will provide a comprehensive resource for the background knowledge required to work in isogeny-based cryptography, and will be informed by all work packages. The book will be published formally with an academic publisher in the last year of the Action.

**D7, Month 48. Final press release.** This press release will give an overview what the Action achieved during the course of the Action, focusing on impact. The press release will also point readers towards the official website and other resources created during the course of the Action where they can learn more about our research.

### 4.1.3 Risk analysis and Contingency Plans

**Scientific and technological risks.** Through its training and dissemination activities, the Action aims to facilitate and increase adoption of isogeny based technologies in industry. Several scientific and technological risks may however adversely impact this goal.

Isogeny based cryptography holds some key advantages over competing technologies:

* Small key, ciphertext and signature sizes, compared to other post-quantum candidates.
* Efficient instantiations of rare or unique post-quantum primitives, such as non-interactive key exchange.
* Instantiations of rare or unique time delay (non-post-quantum) primitives such as Verifiable Delay Functions or Delay Encryption.

Thanks to scientific and technological developments, some of these advantages may dwindle or vanish: non-isogeny-based alternatives with better features may be discovered, or newly discovered attacks may require to increase parameters of some isogeny-based schemes, reducing efficiency.

To mitigate these risks the Action will work on the widest possible portfolio of isogeny based schemes, thus maximising the probability that at least some isogeny based schemes will retain their advantages over competitors.

Of course, diversification will not protect against *black swan* events such as the discovery of a devastating attack, invalidating all isogeny based cryptography at once. However, thanks to the inclusiveness of the network, such a devastating discovery is more likely to come from work done within the Action than outside of it. Thus the Action will have entirely fulfilled its mission of assessing the security of isogeny based cryptography, although with a somewhat disappointing conclusion.

The most likely scenario is somewhere in the middle: the Action will discover some attacks, impacting some isogeny based schemes to some degree, will suggest appropriate corrective measures to keep the schemes safe, and foster a more secure adoption of isogeny based cryptography by industry.

**Internal risks.** Given the size of the network, suboptimal communication among the Action Members and continued isolation of some partners must be proactively addressed.

In the first months of the Action, the Management Committee will mandate a task force to set up and monitor the internal and external communication channels of the Action: mailing lists, social media accounts, websites, chat servers, etc.

Throughout the duration of the action, the involvement of the more isolated Members, especially Inclusiveness Target Countries, will be encouraged by entrusting them with the responsibility of organising events locally. Short Term Scientific Missions will also be used to reduce the isolation of these partners.

Participation statistics will be collected during Training Schools and workshops, and regularly analysed by the Action Management Committee. Shall the statistics indicate a reduced participation by some Action Members, the Management Committee may decide to take additional corrective measures in order to boost engagement.

**External risks.** The success of isogeny based cryptography is somewhat tied to the success of SIKE in the NIST competition. If SIKE were not to be standardised, the popularity of isogeny based cryptography is likely to take a hit, driving adoption down.

The mitigation is again to diversify the portfolio, ensuring that, even if SIKE fails to convince stakeholders, other isogeny based schemes may still succeed.

**Travel restrictions.** Given the current situation, the risk of persistent global difficulties for travelling and organising in-person events cannot be underestimated. The Action Management Committee will act rapidly by publishing Deliverable 2, a series of recommendations addressed to all Action Members for organising virtual events, thus helping maintain a sustained level of collaboration, despite continuing travel difficulties.

Shall the global situation revert back to normal by the start of or during the Action, such recommendations shall still serve as useful guidelines to help increase participation through hybrid events which smoothly support remote participation.

### 4.1.4 GANTT Diagram