Project PROMETHEUS
PRivacy preserving pOst-quantuM systEms
from advanced crypTograpHic mEchanisms
Using latticeS

D2.2

Dissemination plan

Contractual submission date Month 3	Actual submisision date 16/04/2018
Deliverable version 1.0	Main author Laurent Grémy (ENS DE LYON)

`http://prometheuscrypt.gforge.inria.fr`

🐦 h2020prometheus

PROMETHEUS project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780701. The contents of this deliverable are the responsibility of the PROMETHEUS consortium, and do not necessarily reflect the official views of the European Union.

Document information

Grant agreement no.	780701
Project acronym	PROMETHEUS
Project full title	PRivacy preserving pOst-quantuM systEms from advanced crypTograpHic mEchanisms Using latticeS
Type of action	Research and Innovation Action (RIA)
Topic	H2020-DS-06-2017-Cybersecurity PPP: Cryptography
Project dates	1st January 2018 (Month 1) / 31st December 2021 (Month 48)
Duration	48 months
Project URL	`http://prometheuscrypt.gforge.inria.fr`
EU Project Officer	Carmen Ifrim
Work package	WP2 – Dissemination, standardisation and exploitation
Deliverable title	Dissemination plan
Deliverable no.	D2.2
Deliverable version	1.0
Deliverable filename	PROMETHEUS-780701_D2.2.pdf
Nature of deliverable	Report
Dissemination level	Public
Number of pages	16
Responsible partner	ENS DE LYON (participant number 1)
Author	Laurent Grémy (ENS DE LYON)

Abstract. Dissemination is needed for the communication of the project and its results to the internal audience, the scientific community, and the potential business users of the outcomes of the project. Hence all partners are aware and committed to communicate broadly about the project results. It is the principle of all dissemination activities to use research results to create value within the targeted communities of the European Union, to ensure government funding for further advancements, and to maintain the leading edge within the global market place. Wherever possible, research results will be communicated for external awareness creation and knowledge building within the targeted user and scientific communities of the European Union. The communication should guide and create awareness among users for the benefits and potentials of the expected outcomes of PROMETHEUS. In order for the dissemination to be effective, we will describe in this document some ways to coordinate and some media used for the dissemination activities. We will also give the targeted audiences who may benefit of this dissemination process as well as some specific actions for these audiences.

Keywords: Dissemination, communication.

Signatures

Written by	Laurent Grémy	ENS DE LYON	16/04/2018
Reviewed by	Adeline Roux-Langlois	UR1	30/03/2018
Reviewed by	Olivier Sanders	ORANGE SA	04/04/2018
Approved by	Benoît Libert as Project coordinator	ENS DE LYON	04/04/2018
Approved by	Sébastien Canard as Work Package leader	ORANGE SA	13/04/2018

Partners

ENS DE LYON	ENS de Lyon
ORANGE SA	Orange SA
CWI	Stiching Centrum Voor Wiskunde En Informatica
IBM	IBM Research - Zurich
RHUL	Royal Holloway, University of London
RUB	Ruhr-Universität Bochum
SCYTL	Scytl Secure Electronic Voting, S.A.
TCS	Thales Communications & Security S.A.S.
TNO	TNO
UPC	Universitat Politècnica de Catalunya · BarcelonaTech
UR1	Université de Rennes 1
WEIZMANN	Weizmann Institute of Science

Acronyms

CFRG	Crypto Forum Research Group of the IRTF
COST	European Cooperation in Science and Technology
DFG	Deutsche Forschungsgemeinschaft (German Research Foundation)
EPSRC	Engineering and Physical Sciences Research Council
ERC	European Research Council
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IRTF	Internet Research Task Force
ISO	International Organization for Standardization
NIST	US National Institute for Standards in Technology

Contents

1 Communication and dissemination organisation

1.1 Purpose

Dissemination and exploitation activities are considered key enablers for the success of the PROMETHEUS project. The overall aim of these activities is to use research results in order to create value within all participating organisations, thus improving their competitive advantage. Wherever possible, research results will be used for the creation and support of new products, services or processes and will substantially contribute to the benefit of the targeted constituents. Research is meant to create an impact on the society. The PROMETHEUS project aims to disseminate and exploit its results to the community and spread the word about its novelty improvements in the security and privacy of the users.

Since the PROMETHEUS project relies on a consortium of both industrial and academic partners, it is very important to take advantage of this plurality for broadcasting each novelty to all communities. To do so, a common and widespread plan to demonstrate results is necessary to find the right audience and suitable channels for each action. This is the purpose of the present Dissemination Plan.

1.2 Activities

The dissemination plan concerns the planning, monitoring and encouragement of the project's dissemination activities. The dissemination activities will start right after the initiation of the project and will run throughout its lifecycle. The most recognised dissemination activities are:

- establishment and maintenance of the project's website (see Deliverable 2.1);
- participation and presentation of the project and its results in international conferences and workshops;
- scientific publications in journals (mostly open access peer-reviewed articles with storage on appropriate repository);
- continuous collection of all dissemination, cooperation and communication activities of the project and dissemination of these activities via the website and social media in order to raise public awareness of the project and its results;
- intra project communications and transfer of knowledge both within and outside the consortium. This knowledge transfer will be achieved through the setup and maintenance of a project internal communication infrastructure including the collaboration information technology applications, such as Subversion document repository, mailing lists, etc.

These dissemination activities will be organised to communicate the project's results to the wide public, inform society and scientific community as well as promote the exploitation of the PROMETHEUS main components and exploitable products. These goals are in accordance with the articles 29 and 38 of the Grant Agreement.

All partners will contribute in a wide range of dissemination activities. These activities will be coordinated by the Dissemination Manager (see Section 1.3), centralized on the website of PROMETHEUS and disseminated thanks to appropriate media (social media, RSS feeds, ...) in order to maximise the visibility of all the informations.

1.3 Policy

The Dissemination Manager, Adeline Roux-Langlois (UR1), will be in charge of the coordination of the communication and dissemination activities. The Dissemination Manager will be helped partially by the Project Manager, Laurent Grémy (ENS DE LYON), since he will be involved in the quality management process, see Deliverable 1.1 at month 6. In particuluer, all the disseminations activities (e.g., by blog posts on the website, by deliverables, ...) will respect the quality management process, which is maintained by the Project Manager. Additionally, the Work Package 2 leader (ORANGE SA) will also be greatly involved in this dissemination process. Finally, all the partners of the project will take in charge, depending on their participation to specific tasks, the dissemination of the results, see Section 3 about the role of the partners. Since the website of PROMETHEUS is the main entry point of the project on the web, it will collect and archive or give links to all the information related to PROMETHEUS and disseminations activities by partners (job offers, blog posts, articles, events, ...).

All the publications of the twelve PROMETHEUS partners will abide to the articles 29.4 and 38.1.2 of the Grant Agreement as:

- for research articles, with the sentence “This work/The research of *XXX* was supported by the European Union PROMETHEUS project (Horizon 2020 Research and Innovation Program, grant 780701).” in the acknowledgements of the articles;

- for infrastructure, equipment and major results, with the sentence “This *infrastructure / equipment / type of result* is part of the PROMETHEUS project that has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 780701.”;

- for deliverables and communication activities, with the sentence “PROMETHEUS project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 780701.”;

- for public deliverables or communication, by adding in addition to the previous sentence in order to abide to article 38.1.3: “The contents of this *type of the document* are the responsibility of PROMETHEUS consortium, and do not necessarily reflect the official views of the European Union.”.

In addition, the communications in the two last cases (and if possible in the second case about infrastructure, equipment and major results) will also mention the full name of the project, i.e., PRivacy preserving pOst-quantuM systEms from advanced crypTograpHic mEchanisms Using latticeS, the url of the website (curently `http://prometheuscrypt.gforge.inria.fr`) and the European Union’s emblem. Each public deliverable will also start with an executive summary of the results.

During the four years of the project, the Dissemination Manager and the Project Manager will be greatly involved in the dissemination process (see Deliverable 1.1 about quality management for details). This will allow to maximise the impact of the dissemination activities, avoid overlaps as well as the leakage of confidential information and have a unify way to communicate to a broad audience. To do so, partners will always inform at least the Dissemination Manager and the Project Manager about their intention to disseminate. Discussion with all the involved partners will help choose the best way to disseminate. Since PROMETHEUS uses a large number of media to communicate (see Section 2.2.2), there will always exist one or several solutions to maximise the dissemination.

The format chosen to communicate results must be readable by a large audience. This is why every public report deliverable must be a PDF file (if adapted), web pages must follow the main requirement of the World Wide Web Consortium about HTML format, and other appropriate (open) format depending on the communication.

2 Strategy

2.1 Audience

Dissemination activities ensure the visibility and awareness of the project and support the widest adoption of its results among potential users. For PROMETHEUS, the following user groups have been identified as stakeholders and beneficiaries of the project impacts: commercial information and communication technologies (ICT) service providers, research organizations active in the context of cryptography and privacy, standards organizations dealing with cryptography and privacy, and stakeholder groups from use case specific domains, such as e-voting, e-consumer, identity management or threat intelligence.

Another main audience is the general public. Cryptography (with a special focus on quantum-resistant techniques), privacy and security are topics addressed by PROMETHEUS, which are hot topics in the debates concerning web directions. Informing the public and end users about research advances will help explain the benefits of the PROMETHEUS project. For this audience, dissemination should focus on the global concept of the theoretical and mostly practical results. We will also particularly try to provide educational ways to explain our main concept to non technical general public.

2.2 Media

2.2.1 Scientific publications

The scientific audience targeted by the dissemination activities of PROMETHEUS includes the fields of computer science, more specifically security with an obvious focus on cryptography and privacy. It also includes some conferences and workshops more related to specific use cases. The following list contains a sample of relevant recurring scientific conferences: CRYPTO, EUROCRYPT, ASIACRYPT, ACM CCS (conference on Computer and Communications Security of the Association for Computing Machinery), PKC (Public Key Cryptography), TCC (Theory of Cryptography Conference), ESORICS (European Symposium on Research in Computer Security), Financial Crypto, PQCrypto (conference on Post-Quantum Cryptography), E-VOTE-ID (conference on Electronic Voting), ICEDEG (International Conference on eDemocracy & eGovernment) and IEEE (Institute of Electrical and Electronics Engineers) Workshop on Information Forensics and Security.

Open-Access Policy. The consortium reviews the provisions of "The Guidelines on Open Access to Scientific Publications and Research Data" in Horizon 2020 and aligns a strategy for knowledge management and protection. The partners are committed to make available all publications supported by the project as "green" open-access. Green open-access is also known as self-archiving and means that authors upload a preprint or a (potentially revised) author version of their publication at an institutional or subject repository that allows public access. If permitted, this may also be the publisher's version. If possible, the consortium members will also publish in open-access venues ("gold" open access). The choices will be determined by the most appropriate audience to reach, depending on the specific content of publications.

2.2.2 Web visibility

During the lifetime of the project, we will use a website as well as some social media for web visibility. Scientific dissemination activities on the web are deployed around two popular media:

- blog posts for long explanations and short messages about current issues,
- a Twitter account to publish news about events, results and relevant news coming from other entities.

These two media, mainly coordinated by the Dissemination Manager, will be regularly updated. Hence, there is a considered and articulated strategy and a set of identified mechanisms for ensuring that stakeholders, policy makers, practitioners, civil society organisations, media as well as fellow researchers, are all fully kept informed about the activities and results of the project.

The blog is hosted on the website of the PROMETHEUS project, reachable at `http://prometheuscrypt.gforge.inria.fr` (temporary url) and will be continually updated by the members of the project, as defined in Deliverable 2.1.

2.2.3 Press

During the lifetime of the project, we will publish blog posts to inform about the milestones reached by the project and also new scientific developments on topics related to PROMETHEUS. Important blog posts may be the starting point to publish press releases sent to online press agencies or to dedicated press offices (such as those of the CNRS, local press, ...). The communication services of the different members of the project will also help to target the best options for press dissemination.

2.2.4 Events

Scientific and industrial audience. Participation in or organisation of well-known conferences, fairs or meetings within the cryptography and privacy sectors will help us publicising general information, building partnerships as well as directly targeting different audiences. At those occasions the project partners will do presentations, give talks and present posters to increase awareness.

We plan to participate in many workshops and conferences to present our results (see Section 2.2.1). A technical audience (industry) will be reached by participating in and promoting PROMETHEUS at events and publications of the following organizations: European Network and Information Security Agency (ENISA), Networked European Software and Services Initiative (NESSI), national security agencies and more.

We will organize at least two schools and one workshop, related to the technical subjects of the project. These events will be co-organised by several partners of PROMETHEUS. For wide dissemination purposes, some workshops will be opened to whoever is interested in cryptography or in security and privacy. Everyone in the industry, academia or standardization bodies will be welcome to attend, regardless of their status (student or non-student), activity (researcher, developer, lawyer, ...), citizenship or country of residence.

Non-scientific audience. A special attention will also be paid to promote new cryptographic techniques based on lattices and dedicated to privacy-preserving purpose to non-specialists. Such audience will be reached by the means of "Science Festival" (e.g., in France) or by some special dedicated workshops. In front of such an audience, the didactic aspect will be more particularly taken into account, in order to be able to explain very simply PROMETHEUS subject and results.

2.3 Contribution to standardisation and NIST process

One important topic of the dissemination plan is the role of PROMETHEUS' partners in standardisation.

2.3.1 NIST competition

The US National Institute for Standards in Technology (NIST) has organized a call for proposals dedicated to the standardisation of post-quantum secure cryptographic primitives, including signature and encryption mechanisms (see `https://csrc.nist.gov/Projects/Post-Quantum-Cryptography` for details). Even if the the PROMETHEUS project started too late to response to this call, some partners of the consortium (in an independent way) have submitted proposals, and the project will support these ones, as well as study, implement and try to cryptanalyze some of the proposals that have been submitted by the whole cryptographic community.

Inside PROMETHEUS consortium, nine schemes have been submitted to the NIST competition. Some of them are lattice-based and will be particularly followed during the project. Some others (those in italic below) are based on other post-quantum cryptographic methods.

- *BIKE* involves Tim Güneysu (RUB, code based).
- CRYSTALS-DILITHIUM involves Vadim Lyubashevsky (IBM), Léo Ducas (CWI), Eike Kiltz (RUB), Gregor Seiler (IBM) and Damien Stehlé (ENS DE LYON).
- CRYSTALS-KYBER involves Léo Ducas (CWI), Eike Kiltz (RUB), Vadim Lyubashevsky (IBM), Gregor Seiler (IBM) and Damien Stehlé (ENS DE LYON).
- FALCON involves Thomas Prest (TCS), Pierre-Alain Fouque (UR1), Vadim Lyubashevsky (IBM) and Gregor Seiler (IBM).
- FrodoKEM involves Léo Ducas (CWI).
- *GeMSS* involves Gilles Macario-Rat (ORANGE SA, multivariate based).
- LIMA involves Martin Albrecht (RHUL) and Kenny Paterson (RHUL).
- NewHope involves Léo Ducas (CWI).
- *NTS-KEM* involves Martin Albrecht and Kenny Paterson (RHUL, code based).

2.3.2 Other standardisation processes

In parallel to the NIST process, some other organisations have started to take a look at post-quantum cryptography.

The Internet Research Task Force (IRTF) and the Internet Engineering Task Force (IETF) have a growing interest in post-quantum algorithms that are suitable for deployment in Internet protocols. Specifically, the Crypto Forum Research Group (CFRG) of the IRTF is tasked with providing long-term advices to the IETF on the issue of selection of cryptographic algorithms for secure protocols like TLS, SSH and IPsec. The current co-chair of CFRG is Kenny Paterson (RHUL).

In addition, the European Telecommunications Standards Institute (ETSI) has recently created a Cyber Working Group for Quantum-Safe Cryptography, whose a member is Martin R. Albrecht (RHUL). ORANGE SA is also following it. This group will make assessments and recommendations on the quantum-safe cryptography proposals taking into account real-world deployments for various application domains.

Finally, the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) organization has recently launched a Study period which has given the creation of a Standing Document (SD8) on Post-Quantum Cryptography.

Moreover, the recent adoption by the ISO/IEC of some privacy-preserving cryptographic protocol such as group (ISO/IEC 20008-2:2013) and blind (ISO/IEC 18370:2016) signatures shows that the domain studied by PROMETHEUS is of prime importance. In that context, we will follow the evolution of such standards to consider the case of post-quantum mechanisms, putting in one study the initiative of both the NIST and the ISO/IEC organizations. In particular, Jacques Traoré (ORANGE SA) has been the editor of the ISO/IEC 18370:2016 and will follow the evolution of post-quantum cryptography in ISO/IEC.

2.4 Related projects

PROMETHEUS will naturally be built on results from a number of projects in the areas of cryptography, post-quantum cryptography and privacy-preserving techniques. It is obviously the case for relevant projects for which partners are already involved, but also for projects that addressed similar topics as PROMETHEUS and offer an added value to the PROMETHEUS work. Dissemination with some of these projects may help to increase the visibility of the PROMETHEUS results, from an academic but also an exploitation perspective (to be developed in Deliverable 2.3 and 2.4).

2.4.1 Inside the consortium

We first give the list of ongoing projects in which one or several members of PROMETHEUS are involved. We distinguish European projects and then national ones.

European projects. The European projects linked with PROMETHEUS and involving PROMETHEUS participants are the following.

ERC ALGSTRONG CRYPTO. The ERC "Algebraic Methods for Stronger Crypto" is held by Ronald Cramer (CWI) for five years (2017-2022). The research in this project focuses on a suite of generalisations of the notion of an "arithmetic codex" and their broad applications in cryptology, including (quantum-safe) public-key encryption and multiparty computation. PROMETHEUS will exploit results from this project on the codex-primitive and its generalizations and apply them in particular to the design of practical quantum-safe zero knowledge proofs.

ERC ERCC. The ERC "Efficient Resource Constrained Cryptography" is held by Eike Kiltz (RUB) for five years (2014-2018). ERCC focuses on efficient cryptography on resource-constrained devices. Due to their great efficiency, part of the ERCC project considers lattices. However, this is done in context of small devices, where memory consumption, execution time, and other factors are limited. The expertise accumulated in the ERCC project will be of great use as input for Work Package 3 and Work Package 4. There are some overlapping parts with FELICITY.

ERC FELICITY. The ERC "Foundations of Efficient Lattice Cryptography" is held by Vadim Lyubashevsky (IBM) for five years (2016-2020). The main focus of FELICITY is to create the foundational building blocks for lattice-based cryptography. The grant was obtained under the 2014 call for ERC starting projects, but is currently funded by the Swiss National Science Foundation. This is due to the fact that the PI moved to Switzerland, which was not a participant in the 2014 call.) There are some overlapping parts between FELICITY and the current proposal. Both projects deal with constructing practical lattice-based primitives. The main difference between the two projects is that the PROMETHEUS is use-case driven while the goal of FELICITY is to construct general building blocks, the current proposal will focus more on very specific applications, which may require constructions that have no equivalents in classical cryptography. FELICITY is not concerned in building e-voting, digital cash, or general anonymous credential schemes, which are at the core of the current proposal.

ERC LattAC. The ERC "Lattices: Algorithms and Cryptography" is held by Damien Stehlé (ENS DE LYON) for five years (2014-2018). LattAC focuses on lattice-based cryptography and lattice algorithms. The lattice-based cryptography component is upstream of PROMETHEUS. It tackles the hardness foundations of lattice based cryptography (how hard are the underlying computational problems?) and attempts to determine its expressivity (which types of cryptographic primitives are possible with standard lattice hardness assumptions?). The expertise accumulated during that project will be an asset for PROMETHEUS, in particular for Work Package 3, and, to a lesser extent, Work Package 4.

ERC REACT. The ERC "Realizable Advanced Cryptography" is held by Zvika Brakerski (WEIZMANN) for five years (2017-2022). REACT is a foundational theoretical project that addresses the asymptotic aspects of establishing some recently proposed cryptographic primitives. PROMETHEUS and REACT address different parts of the spectrum of cryptographic research. The goal of PROMETHEUS is to develop practical post-quantum lattice based cryptographic protocols to be used at present time. On the other hand, REACT is a conceptual study of premature cryptographic objects, ones whose very existence is in question, and are not expected to be practical in the next few years.

ICT COST Action. This project is a four years project (April 2014 - April 2018) and is divided in subprojects. The one about "Cryptography for Secure Digital

Interaction" involves Jorge Villar (UPC). The aim of this COST Action is to stimulate interaction between the different national efforts in order to develop new cryptographic solutions and to evaluate the security of deployed algorithms with applications to the secure digital interactions between citizens, companies and governments. The Action will foster a network of European research centers thus promoting movement of ideas and people between partners.

PQCrypto. PQCrypto is a recently closed project (February 2018). It involved Tim Güneysu (RUB) and aims at designing a portfolio of high-security post-quantum public-key systems, and improving their speed, adapting to the different efficiency challenges of mobile devices, cloud, and Internet of Things. The PQCrypto project aims at efficient implementations. PQCrypto solely considers "basic" quantum-secure primitives that shall be used as (drop-in) replacements for plain encryption schemes, digital signatures and key agreement. The PROMETHEUS project targets advanced schemes beyond these basic schemes. PROMETHEUS moreover focuses on lattice-based constructions, while PQCrypto considers several kinds of post-quantum cryptographic techniques.

SAFEcrypto. "Secure Architectures of Future Emerging Cryptography" is a three years project (2015-2018). It involves Tim Güneysu (RUB) and will provide a new generation of practical, robust and physically secure post-quantum cryptographic solutions. It also aims at studying their impact in several use cases such as network security, satellite communications, and cloud. As in PROMETHEUS, SAFECrypto considers the use of lattice-based cryptography in some specific use cases, in particular focusing on the efficient implementation of such tools. PROMETHEUS will certainly make use of SAFECrypto results. However, the PROMETHEUS project plans to go beyond since we aim at focusing on more advanced protocols, which is not the case of SAFECrypto.

National projects. The national projects linked with PROMETHEUS and involving PROMETHEUS participants are the following ones.

CArSD. The project "Criptografía avanzada para afrontar nuevos retos de la sociedad digital" (Advanced Cryptography to face new challenges in the eSociety) is led by Javier Herranz (UPC) for three years (2017-2019). The project is about cryptographic protocols (homomorphic encryption, group key establishment, attribute-based cryptography, cryptography for eVoting), distributed cryptography (secret sharing, distributed cryptographic protocols) and post-quantum cryptography (lattice-based cryptography, mainly).

EPSRC. The EPSRC "Bit Security of Learning with Errors for Post-Quantum Cryptography and Fully Homomorphic Encryption" is held by Martin R. Albrecht (RHUL) for two years (2017-2018). The project looks at the cost of solving the "Learning With Error" problem concretely for both post-quantum cryptography and full-homomorphic encryption.

EQUIP. This project involves RHUL. This project aims to look at hybrid post-quantum / classical / quantum key distribution protocols.

DFG. The DFG "Implementierungsaspekte alternativer asymmetrischer Kryptoverfahren" (Implementation aspects of alternative asymmetric cryptographic methods) involves and was held up to August 2017 by Tim Güneysu (RUB), and now held by Rolf Drechsler (Universität Bremen). The project investigates implementation properties of four types of post-quantum cryptographic approaches, which are hash-based, code-based, (ideal) lattice-based and multivariate quadratic and cryptography.

RISQ. RISQ stands for "Regroupement de l'Industrie française pour la Sécurité Post-Quantique" (French Industry consortium for the post-quantum security) and involves TCS, ENS DE LYON, UR1 and ORANGE SA for three years (2017-2019). Its main goal is to prepare the French security industry to the post-quantum transition. It only considers basic cryptographic primitives (i.e., ordinary encryption, signature schemes and key exchange protocols) without advanced properties. Lattice-based is one of the quantum-resistant families of cryptosystems studied in this project.

2.4.2 Outside the consortium

We now give the list of projects which we think are related to ours. We differentiate the projects that are now finished and the ones that are ongoing.

Ongoing projects. We first focus on ongoing projects. For these ones, we may interact with them in order to find some common studies. We will contact them so as to see the best way to proceed[1].

FutureTPM. The goal of FutureTPM is to design, implement and evaluate a quantum-resistant trusted platform module (a secure cryptoprocessor).

New Post-Quantum Cryptographic Constructions. Funded by the Singapore Ministry of Education, this project aims at building post-quantum cryptographic primitives for anonymity. These primitives can be lattice-based, similar to the PROMETHEUS project, but also code-based[2].

Ended projects. We finally give the list of some projects that are ended but which may give some inputs to PROMETHEUS. The results of these projects will be one input of the technical surveys (deliverables D3.1, D4.1 and D5.1).

ABC4Trust. "Attribute-based Credentials for Trust" aims at advancing the federation and interchangeability of technologies supporting trustworthy and at the same time privacy-preserving attribute-based credentials. The ABC4trust project was focused on building anonymous credentials from classical assumptions. Part of the PROMETHEUS project aims to extend these constructions so as to make them quantum-secure.

ECRYPT and ECRYPT II. These two projects were European ECRYPT II Network of Excellence for Cryptology. Their objectives were to intensify the collaboration of European researchers in information security and cryptology. These projects developed and strengthened a European-wide network of researchers in cryptography, establishing long-term collaborations at a researcher-to-researcher level, and establishing relationships on which future funding bids have been built, including the PROMETHEUS project.

[1] We note here that this has already been the case with the FutureTPM Horizon 2020 project.

[2] Benoît Libert (ENS DE LYON) is an external collaborator of this project.

EKSISTENZ. The goal of EKSISTENZ is to reduce identity theft in Europe, while accounting for citizens' privacy, by developing cryptographic tools. PROMETHEUS will develop post-quantum systems which enable protecting privacy within similar services. PROMETHEUS will be built on the experience of cryptographically protecting privacy within electronic services.

HEAT. The HEAT project develops advanced cryptographic technologies to process sensitive information in encrypted form, without needing to compromise on the privacy and security of the citizens' and organizations' input data. The HEAT project is dedicated to fully homomorphic encryption, which is only a minor topic in PROMETHEUS. The outcomes of HEAT will be used as a basis for PROMETHEUS regarding cryptographic constructions and studied use cases.

PRACTICE. PRACTICE has worked on a secure cloud framework which allows computation on encrypted data. The PRACTICE project is dedicated to advanced encryption techniques, which is only one topic in PROMETHEUS. As for HEAT project, the outcomes of PRACTICE will be used as a basis for PROMETHEUS.

WITDOM. This project deals with secure computation on outsourced health and financial data. This very slightly overlaps with the fully-homomorphic encryption task of PROMETHEUS.

3 Role of the partners

We now give the specific role of each partner in this dissemination plan.

At first, we note that all partners will contribute to the dissemination of the results of the project by participating in the writing of scientific papers and by giving scientific talks to a quite broad audience. We now details other specific actions.

3.1 ENS DE LYON

ENS DE LYON prepared the present dissemination plan for the planning, the monitoring and the encouragement of the project's dissemination activities. It has also provided and will maintain the project website (see Deliverable 2.1 and Section 2.2.2).

3.2 ORANGE SA

ORANGE SA will lead the Work Package 2 and Task 2.1 on exploitation and innovation management. ORANGE SA will also contribute to Task 2.3 on standardisation, providing guidance on relevant standardisation bodies where the project's results may be contributed to influence the state of post-quantum and privacy-preserving cryptographic mechanisms (in particular with ISO/IEC). ORANGE SA will also contribute to the dissemination and exploitation by publicising PROMETHEUS research results, but also making them available as potential industrial solutions. ORANGE SA will participate to workshops on the transitions to use quantum-safe cryptography, mainly dedicated to companies (such as the ones proposed by TNO in Section 3.9) and will also promote lattice-based cryptography to non-scientific public in educational workshops.

3.3 CWI

CWI will contribute to Task 2.3 by providing a digest of the conclusion on cryptanalysis (Task 3.3) and an assessment of the asymptotic and concrete security of the candidates to the NIST process (see Section 2.3). On Task 2.1, CWI will contribute to the open-source software FPLLL (`https://github.com/fplll/fplll`), and potentially prototypes of new fully homomorphic encryption schemes (Task 4.2). Concerning dissemination (Task 2.2), CWI will participate to conferences and workshops, but could also be interested in organization of summer/winter schools.

3.4 IBM

IBM has submitted several proposals to the NIST process on standardisation of post-quantum primitives. During the running time of this project, IBM will participate in the ongoing discussions regarding the submissions.

3.5 RHUL

RHUL will contribute to Task 2.2 by maintaining information on all research outputs on the project website. RHUL will lead Task 2.3, coordinate the involvement of project partner in the NIST process, and ensure a smooth flow of information back to the project members from the NIST process. RHUL will also lead for the project in working with the Internet Engineering Task Force (IETF).

3.6 RUB

RUB will make the link between PROMETHEUS and other ongoing projects in which it is involved.

3.7 SCYTL

SCYTL will contribute to the overall exploitation, dissemination and standardisation activities to be undertaken within the domain of the project. Specifically, SCYTL will address scientific and private-sector end-user communities, the public sector and the wider public. To pave the way for exploitation, SCYTL will also establish valuable end-user contacts and groups of interest around the project and its results.

3.8 TCS

TCS has proposed a post-quantum scheme to the NIST process and will then provide support for it. TCS will also contribute to internal and external disseminations through presentations and publications.

3.9 TNO

TNO will contribute to dissemination by giving presentations on the project results to a broad audience. The technology developed within the use case "Cyber Threat Intelligence" (see Work Package 6) will be disseminated towards potential users within the Netherlands. In addition, TNO is considering to organize one or more workshops towards the end of the project, to help companies understand the transitioning process towards quantum-safe cryptography.

3.10 UPC

UPC will contribute to the dissemination by additionally organizing summer/winter schools related to PROMETHEUS topics.

3.11 UR1

UR1 will contribute to Task 2.3 by providing feedback from side-channel analysis on NIST candidates and by being involved in the Crypto Forum Research Group (CFRG) of the Internet Research Task Force (IRTF). UR1 will participate to conferences and workshops and by organizing a workshop. UR1 will also participate actively to Task 2.2, especially in the coordination and the strategy about the dissemination activities, since the Dissemination Manager (Adeline Roux-Langlois) is a member of UR1. For this task, UR1 will closely collaborate with ORANGE SA, the leader of the Work Package 2, and ENS DE LYON, see Section 1.3.

3.12 WEIZMANN

WEIZMANN will participate in conferences and workshops in order to disseminate and publicise the products of conducted research, as well as give lectures in leading research organizations.

4 Conclusion

This dissemination plan has presented an overview of the PROMETHEUS dissemination strategy, media and actions during the four years of the project. This dissemination plan is highly adaptable, since in four years, new media can become unavoidable, some other may be less attractive or less usable and some new actions, not considered in this document, may become valuable in a near future. It can be seen as a first list of potential actions that will be taken by the members of the consortium to promote our results.