D2.4 Annual Dissemination Report & Material Y2

Document Identification			
Status	Final	**Due Date**	31/12/2019
Version	1.0	**Submission Date**	18/12/2019

Related WP	WP2	**Document Reference**	D2.4
Related Deliverable(s)	D1.1, D1.4, D2.1–D2.3, D2.5, D2.8–D2.15	**Dissemination Level(*)**	PU
Lead Participant	UH	**Lead Author**	Kimmo Järvinen (UH)
Contributors	All partners	**Reviewers**	Wim Vandevelde (KU Leuven)

Keywords:

Dissemination, Publications, Events, Conferences, Standardization, Project Advisory Board

This document is issued within the frame and for the purpose of the FENTEC project. This project has received funding from the European Union's Horizon2020 under Grant Agreement No. 780108. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission.

(*) Dissemination level.-PU: Public, fully open, e.g. web; CO: Confidential, restricted under conditions set out in Model Grant Agreement; CI: Classified, Int = Internal Working Document, information as referred to in Commission Decision 2001/844/EC.

Document Information

List of Contributors	
Name	Partner
Kimmo Järvinen	UH
Alicia Cuadrado Cordero	Atos
Francisco Gala	Atos
Azam Soleimanian	ENS
Clément Gentilucci	FUAS
Yolan Romailler	KUD
Danaja Fabčič Povše	KU Leuven
Svetla Nikova	KU Leuven
Hendrik Waldner	UEDIN
Norman Scaife	WALLIX
Miha Stopar	XLAB

Document History			
Version	Date	Change editors	Changes
0.1	09/10/2019	Kimmo Järvinen (UH)	ToC and general text
0.2	04/12/2019	Kimmo Järvinen (UH)	More details added
0.3	09/12/2019	All partners	Partner specific texts
0.4	10/12/2019	Kimmo Järvinen (UH)	Draft for internal review
1.0	18/12/2019	Kimmo Järvinen (UH)	Final version

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable Leader	Kimmo Järvinen (UH)	18/12/2019
Technical Manager	Michel Abdalla (ENS)	18/12/2019
Quality Manager	Diego Esteban (ATOS)	18/12/2019
Project Coordinator	Francisco Gala (ATOS)	18/12/2019

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
ABE	Attribute Based Encryption
ACM	Association for Computing Machinery
ARI	Atos Research and Innovation department
CS	Computer Science
ECC	Elliptic Curve Cryptography
EU	European Union
ESOCC	European Conference on Service-Oriented and Cloud Computing
ETSI	European Telecommunications Standard Institute
IACR	International Association for Cryptologic Research
IBE	Identity Based Encryption
IEEE	Institute of Electrical and Electronics Engineers
IFIP	International Federation for Information Processing
ISO	International Organization for Standardization
KPI	Key Performance Indicator
NIST	National Institute of Standards and Technology (of United States)
PAB	Project Advisory Board
RSA	Rivest-Shamir-Adleman public-key cryptosystem
WP	Work Package
Y1	Year 1 (2018)
Y2	Year 2 (2019)
Y3	Year 3 (2020)

Executive Summary

In this deliverable D2.4 “Annual Dissemination Report & Material Y2”, we present a summary of dissemination activities of FENTEC during the second project year (Y2) from January 2019 (M13) to December 2019 (M24). The deliverable focuses on the scientific activities and outcomes of FENTEC by presenting scientific publications and event participations. The communication activities and outcomes are not in the scope of this deliverable as they are discussed in D2.9 “Annual Communication Activities Report Y2”. In addition to the scientific outcomes, this deliverable also presents overviews of standardization and PAB activities. We also update the dissemination plan of FENTEC for the third project year (Y3) from January 2020 (M25) to December 2020 (M32). The original dissemination plan was described in D2.2 “Dissemination Plan” submitted in June 2018 (M6) and the annual dissemination report for the first project year (Y1) was published as D2.3 in December 2018 (M12).

To summarize, the dissemination outcomes during Y2 included:

- 12 scientific publications (11 published and 1 accepted);
- 8 other publications (2 in English and 6 in Spanish); and
- 8 events attended.

Additionally, FENTEC has been active with relevant standardization bodies and held one online PAB conference during 2019. All KPIs for dissemination that were set in D2.2 were achieved during Y2. Also standardization and PAB activities are progressing according to the plans.

1 Introduction

1.1 Purpose of the document

This deliverable D2.4 “Annual Dissemination Report & Material Y2” describes the dissemination activities and their outcomes for the first project year Y2, from January 2019 (M13) to December 2019 (M24). This deliverable and the described activities belong to the WP2 of the project titled “Dissemination, Communication, Standardisation and Exploitation” and, in particular, to the following tasks: T2.1 “Dissemination planning and networking”, T2.4 “Standardisation”, and T2.5 “Project advisory board”. The emphasis of this deliverable is on the results of T2.1. The task T2.2 “Communication activities” will be discussed in detail in D2.9 “Annual Communication Activities Report Y1”. T2.4 and T2.5 are also shortly surveyed in this deliverable.

Dissemination material described in this deliverable are scientific publications, press releases, etc. Other material such as brochures, leaflets, web pages, tweets, etc. are counted as communication material and discussed in D2.9. This deliverable will also provide information about events, in which FENTEC members participated, and describe how they connected to the work done in FENTEC during Y2. Further details about the PAB and the outcomes of the second PAB meeting will be provided in D2.14 “Project Advisory Board Workshops Report Y2”. Standardization related issues will be more closely discussed in D2.11 “Preliminary Standardisation Report” [11] that was submitted in M18.

D2.2 “Dissemination Plan” [9] and D2.3 “Annual Dissemination Report & Material Y1” [10] defined KPIs for dissemination, standardization, and PAB for Y2:

- 4 scientific publications, accepted for publication in peer-reviewed conferences or journals;
- 4 presentations, invited talks, and keynotes in scientific conferences, workshops, summer schools, and other events; and
- 5 participations in scientific conferences and workshops.

The standardization KPIs for the entire duration of the project (Y1–Y3) are:

- 3 standardization organizations contacted;
- 1 liaison agreements signed with standardization organizations;
- 3 communication activities with standardization organizations; and
- 2 standardization documents reviewed and commented.

The PAB KPIs for Y2 are:

- 1 PAB meeting or teleconference; and
- 6 PAB members present at a meeting or teleconference.

This deliverable will examine how the KPIs were met and if some specific measures need to be taken in order to improve performance during Y3 regarding the KPIs not met in Y2.

1.2 Structure of the document

This deliverable is structured as follows.

- Section 2 discusses dissemination activities and material and presents standardization and PAB activities done during Y2.
- Section 3 presents the updated dissemination plan for Y3.
- Section 4 ends the deliverable with conclusions and studies how the project performed regarding the KPIs for Y2.

2 Dissemination activities and material

This section describes the dissemination activities and results during Y2. Specifically, the publications are discussed in Section 2.1. Events, in which the FENTEC members participated, and their connections to the project are discussed in Section 2.2. Standardization and PAB related activities are shortly reviewed in Sections 2.3 and 2.4, respectively.

2.1 Publications

The main research outputs of FENTEC are scientific publications published in relevant scientific conferences and journals. During Y2 FENTEC continued to produce scientific results and articles written about them were submitted to leading venues in the field. The venue selection was made according to the guidelines described in D2.2 [9].

Table 1 collects the scientific publications produced by FENTEC that have been either published or have been accepted to be published during Y2. It shows that the total number of scientific publications is 12. All of them have been (or are accepted to be) published in high quality scientific venues in the fields of cryptology, information security, and digital design, such as ASIACRYPT, DAC, CT-RSA, and ESORICS.

The topics of the scientific publications are related either to new functional encryption schemes or relevant building blocks [5, 4, 2, 1, 12, 3], implementation techniques that are relevant also for functional encryption schemes [13], applications of functional encryption [26, 28, 16], or legal aspects [7].

In addition to the scientific publications, FENTEC has published 8 other publications including blog posts and press releases, and media responses to FENTEC's press releases in order to increase the awareness and visibility of the project. Details about the other publications are available in Table 2.

FENTEC is committed to open access publication and all deliverables and scientific publications will be made freely available on the project's website, as far as this is permitted by the copyright policies of original publications. So far, all publications produced by FENTEC have been provided on the website at latest at the time of publication, but some already before that (with "to appear" status). Certain publications have been made available also in IACR Cryptology ePrint Archive, a free-of-charge public online repository for papers on cryptology.

2.2 Participation in scientific events

During Y2, FENTEC members participated in a number of events, most of which were scientific conferences focusing on cryptology and related fields. In these events, the members gave presentations about the work done in FENTEC. This also includes presentations that were given about the scientific publications discussed in Section 2.1. The events, in which FENTEC members participated, are collected in Table 3 and discussed more closely below.

Authors, title, the name of the conference or journal	Status	Partner(s)
Ward Beullens and Hoeteck Wee: "Obfuscating Simple Functionalities from Knowledge Assumptions," **Public-Key Cryptography — PKC 2019** [5]	Published	KU Leuven, ENS
Angshuman Karmakar, Sujoy Sinha Roy, Frederik Vercauteren and Ingrid Verbauwhede: "Pushing the speed limit of constant-time discrete Gaussian sampling. A case study on the Falcon signature scheme," **Design Automation Conference — DAC 2019** [13]	Published	KU Leuven
Ward Beullens, Jean-Charles Faugère, Eliane Koussa, Gilles Macario-Rat, Jacques Patarin and Ludovic Perret: "PKP-Based Signature Scheme," **Progress in Cryptology — INDOCRYPT 2019** [4]	To appear	KU Leuven
Danaja Fabcic: "Protecting Human Rights through a Global Encryption Provision," **Security and Law** [7], Intersentia, Antwerpen, 2019	Published	KU Leuven
Edouard Dufour-Sans and David Pointcheval: "Unbounded Inner-Product Functional Encryption with Succinct Keys," **Applied Cryptography and Network Security — ACNS 2019** [6]	Published	ENS
Michel Abdalla, Fabrice Benhamouda, Markulf Kohlweiss and Hendrik Waldner: "Decentralizing Inner-Product Functional Encryption," **Public-Key Cryptography — PKC 2019** [2]	Published	ENS, UEDIN
Michel Abdalla, Fabrice Benhamouda, Romain Gay: "From Single-Input to Multi-client Inner-Product Functional Encryption," **ASIACRYPT 2019** [1]	Published	ENS
Theo Ryffel, Edouard Dufour-Sans, Romain Gay, Francis Bach, David Pointcheval: "Partially Encrypted Machine Learning using Functional Encryption,"**Advances in Neural Information Processing Systems (NeurIPS 2019)** [26]	Published	ENS
Romain Gay: "Public-Key Encryption, Revisited: Tight Security and Richer Functionalities," **PhD Thesis** [12]	Published	ENS
Manuel Barbosa, Dario Catalano, Azam Soleimania and Bogdan Warinschi: "Efficient Function-Hiding Functional Encryption: From Inner-Products to Orthogonality," **Cryptographers' Track at the RSA Conference — CT-RSA 2019** [3]	Published	ENS
Miha Stopar, Manca Bizjak, Jolanda Modic and Jan Hartman: "emmy: Trust-Enhancing Authentication Library," **IFIP International Conference on Trust Management — IFIPTM 2019** [28]	Published	XLAB
Tilen Marc, Miha Stopar, Jan Hartman, Manca Bizjak and Jolanda Modic: "Privacy-Enhanced Machine Learning with Functional Encryption," **European Symposium on Research in Computer Security – ESORICS 2019** [16]	Published	XLAB

Table 1: Scientific publications by FENTEC during Y2

Title, authors, and other publication details	Publication type	Partner(s)
Obscure meaning, cryptic messages: cryptography and the law [CiTiP website]	CiTiP blog	KU Leuven
Fentec permitirá transmitir datos seguros a través de redes inciertas [Zona Movilidad]	Media response to press release	ATOS
Compartir datos de forma segura a través de redes no seguras [tech News]	Media response to press release	ATOS
Kudelski Security Announces FENTEC Participation to Develop New Functional Encryption Technologies [Kudelski Website]	Press release	KUD
Atos lidera un proyecto europeo que permitirá compartir datos de forma segura a través de redes no seguras [Cyber-Security news]	Media response to press release	ATOS
El proyecto europeo FENTEC desarrollará nuevos sistemas de encriptación [Conectrónica]	Media response to press release	ATOS
Atos lidera un proyecto europeo que permitirá compartir datos de forma segura a través de redes no seguras [Ecnomista de hoy]	Media response to press release	ATOS
Atos Trabaja Para Compartir Datos De Forma Segura A Través De Redes No Seguras [Cloud Computing]	Media response to press release	ATOS

Table 2: Other publications by FENTEC during Y2

Name of the event	Location and date	Partner(s)
The 22nd Conference on Practice and Theory of Public Key Cryptography (PKC 2019) [www]	Beijing, China April 14-17, 2019	KU Leuven, ENS
The 56th Design Automation Conference (DAC 2019) [www]	Las Vegas, United States June 2-6, 2019	KU Leuven
The 17th International Conference on Applied Cryptography and Network Security (ACNS 2019) [www]	Bogotá, Colombia June 5-7, 2019	ENS
The 25th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT19) [www]	Kobe, Japan December 8-12, 2019	ENS
The 33th Annual Conference on Neural Information Processing Systems (NeurIPS19) [www]	Vancouver Canada December 8-14	ENS
The Cryptographers' Track at the RSA Conference (CT-RSA 2019) [www]	San Francisco, CA, USA March 4–8, 2019	ENS
The 13th IFIP WG 11.11 International Conference on Trust Management(IFIPTM 2019) [www]	Copenhagen, Denmark July 17-19, 2019	XLAB
The 24th European Symposium on Research in Computer Security (ESORICS 2019) [www]	Luxembourg September 23–27, 2019	XLAB

Table 3: Conferences and other events where FENTEC participated during Y2

2.2.1 PKC 2019

The 22nd edition of the International Conference on Practice and Theory of Public Key Cryptography (PKC 2019) was held in Beijing (China) in April 2019. PKC is an annual conference with an explicit focus on public-key cryptography, sponsored by IACR, the International Association for Cryptologic Research. Ward Beullens from KU Leuven presented his FENTEC related paper [5]. Also Hendrik Waldner from UEDIN presented the FENTEC related paper [2] in this conference.

2.2.2 DAC 2019

The 56th edition of the Design Automation Conference (DAC 2019) was held in Las Vegas (United States) in June 2019. DAC is the oldest and largest conference in Electronic Design Automation (EDA), started in 1964. Angshuman Kamakar from KU Leuven presented his FENTEC related paper [13].

2.2.3 ACNS 2019

The 17th edition of the International Conference on Applied Cryptography and Network Security (ACNS) was held in in Bogotá, Colombia, from June 5 to June 7 2019. ACNS is an annual conference focusing on current developments that advance the areas of applied cryptography and its application to systems and network security. Its goal is to represent both academic research works as well as developments in industrial and technical frontiers. Edouard Dufour-Sans from ENS presented the FENTEC related paper [6] in this conference.

2.2.4 CT-RSA 2019

The CT-RSA conference, in San Francisco, March 4th-8th 2019, held in conjunction with RSA Conference USA. CT-RSA, or Cryptographers Track RSA Conference, is the venue devoted to scientific papers on cryptography, a great venue to ensure that scientific results not only get published to the wider cryptologic community, but also get exposed to technical attendees from industry, government and wider afield. Razvan Rosie from ENS presented the FENTEC related paper [3].

2.2.5 ASIACRYPT 2019

The 25th edition of the Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT19), is taking place at Japan on December 8-12, 2019. The Asiacrypt conference is an international conference on all aspects of cryptology sponsored by the International Association for Cryptologic Research (IACR) since 2000 in cooperation with the technical group on Information Security(ISEC) of Institute of Electronics, Information and Communication Engineers (IEICE). Romain Gay is presenting the FENTEC related paper [1].

2.2.6 NEurIPs 2019

The 33rd Annual Conference on Neural Information Processing Systems (NeurIPS) is going to be held in Vancouver, Canada from December 8th to 14th, 2019. The purpose of the Neural Information Processing Systems annual meeting is to foster the exchange of research on neural information processing systems in their biological, technological, mathematical, and theoretical aspects. Theo Ryffel from ENS is presenting the FENTEC related paper [26] in this conference.

2.2.7 IFIPTM 2019

The 13th IFIP International Conference on Trust Management (IFIPTM 2019) was held at the Technical University of Denmark (DTU) in Copenhagen, Denmark. The mission of the IFIPTM 2019 Conference was to share research solutions to problems of Trust and Trust management, including related Security and Privacy issues, and to identify new issues and directions for future research and development work. Miha Stopar presented the FENTEC related paper [28].

2.2.8 ESORICS 2019

European Symposium on Research in Computer Security (ESORICS) is the premier European conference on information security. The 24th edition was held in Luxembourg. Tilen Marc presented the FENTEC related paper [16].

2.3 Standardization

During Y2 our main result is our liaison with ETSI, which enables us to actively contribute to the working group Cyber and more particularly to one of the current efforts: Guide to Identity Based Encryption. The document will describe the use and application of IBE. The report is intended to allow non-experts in the technology of IBE to be able to gain an understanding of the technology, its domains of application, and its required environment. In addition, the document reviews use of IBE against more common asymmetric encryption schemes (e.g. RSA and ECC schemes), as well as more generalized ABE schemes. A review of algorithms available to implement IBE and their evolution to quantum safe instances will also be covered. We have already provided input to the document and we have been invited to participate in the next meeting of ETSI when the document will be further discussed.

We have also applied for liaison to ISO SC 27 IT on “Security Techniques” and more specifically to WG 2 on “Cryptography and security mechanisms”, but unfortunately our request has not been considered yet despite our continuous efforts. We are still in contact with ISO through representatives from partners of the consortium (e.g., KU Leuven). Currently our representative at ISO Ward Beullens is working in Working Group 2 of ISO/IEC JTC1 CS27 to produce Standing Document 8 (SD8). This standing document will provide a publicly available general survey on post-quantum cryptography. The purpose is to get WG2 experts familiar with post-quantum cryptography and prepare for standardization. Recently we have also applied to WG 5 “Identity Management & Privacy Technologies”. We are still waiting for the result. We believe we can contribute also to WG5 with proposing relevant use cases for example.

2.4 Project advisory board (PAB)

The second PAB meeting took place online on October 25, 2019, during which the FENTEC partners presented a summary of the work performed during Y2 and the plans for the last project year.

The PAB members present at the call were:

- Prof. Sergey Gorbunov (University of Waterloo, Canada)
- Dr. Antonio Kung (Trialog, France)
- Dr. Ventzislav Nikov (NXP Semiconductors, Belgium)

D2.14 “Project Advisory Board Workshop Reports Y2” (M24) contains more details on the second PAB meeting.

3 Dissemination plans for the next year

This section presents an updated dissemination plan for the third project year Y3, which is also the last year of FENTEC. First, more general plans are discussed in Section 3.1 followed by individual dissemination plans for each partner in Section 3.2.

3.1 General dissemination plan

The detailed plans for disseminating the results of FENTEC presented in D2.2 [9] are still valid and exercised also for Y3 of the project. In the following, we survey certain key aspects, but the reader is referred to D2.2 [9] for a more detailed discussion.

The results of FENTEC are being disseminated via several channels. The public deliverables which will be produced in the project also serve as a dissemination channel, but they are not discussed further in this deliverable (see D1.1 "Work Plan Y1" [8] for a complete list of deliverables).

In addition to the public deliverables, FENTEC also disseminates the most important outcomes of the project by publishing scientific articles in the leading international scientific conferences and journals. In fact, these can be considered as the main dissemination channels for the scientific results of FENTEC because they probably have the highest impact in the scientific communities of cryptography, information security, and cryptographic engineering. Lists of particular scientific conferences and journals are available in Tables 2 and 3 of D2.2 [9], respectively, and they are still perfectly valid also for Y3.

The selection of conferences for publishing scientific articles considers multiple factors including the topic, the quality of peer-review process, the impact in the community, and other issues such as history and reputation. The scientific communities of cryptography, information security, and cryptographic engineering emphasize conference publications more than many other fields of science and, hence, conferences are the main forums to distribute new scientific results. FENTEC will aim to maximize the impact of its results and, hence, the goal is to publish the articles in as many good conferences as is realistically possible (considering the above factors). The emphasis of high-quality conferences is also visible in the outcomes produced during Y1 and Y2 and the same trend will be continued during Y3.

FENTEC continues its commitment to open access publication. Depending on the policies of the selected conferences and journals, the papers are also made available either at same time with the submission or at a later stage (e.g., when published) via the project website and online repositories.

FENTEC disseminates the work done and its results also by giving presentations in conferences and other events. These can be presentations about conference papers, invited talks, keynote talks, lectures in summer schools, etc. Conference and event participation can be regarded as dissemination actions as well, because these enable networking with other experts of the community and, thus, dissemination of the project and its results. Decisions to participate in conferences and other events are made using similar factors that are used in the selection of publication forums.

3.2 Individual dissemination plans

3.2.1 ATOS

As the Project and Innovation Manager, Atos will continue coordinating the communication tasks in FENTEC project and making important efforts in the WP2.

Within the Atos Research and Innovation department (ARI), Atos counts with a specific area specialized on a wider strategic integration of communication and dissemination activities, with an approach to business, called the Innovation Hub. For Y3, the company will go on making available to the project their corporative channels, both internal and external tools, in order to maximize the dissemination and knowledge of the FENTEC results and reach to the public target.

Atos will continue working together with the dissemination team, aiming to adapt the FENTEC messages to every public. From the marketing and communication department in the Innovation Hub, Atos provides several tools and channels with the following structure:

- **Internal:** Atos research mailing lists, ARI public info in Zen space, Atos Research and Innovation Booklet, and internal ARI and Atos newsletters.
- **External:** The group has direct contact with Iberia and Global marketing department to distribute Press releases and general content through media or the newsroom. Also, we dispose of ARI Marcomm social Media, Atos Spain Social Media, ARI Digital Show (ARI annual event), ARI Booklet, Potential participation in industrial events, or Atos Thought Leadership Blog. These are visualized in Figure 1.

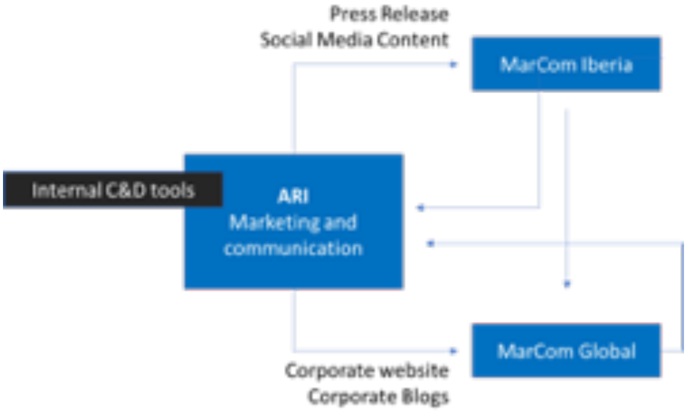

Figure 1: Atos dissemination channels

3.2.2 ENS

ENS will continue to use internal and external communication channels, such as group meetings, department meetings, and the ENS Crypto mailing list, to promote FENTEC within ENS and in France.

As in the first two years, dissemination towards the broader research community will continue to be done through the publication of scientific papers in top international conferences and journals in the areas of cryptography and security. These include the IACR general conferences (CRYPTO, EUROCRYPT, ASIACRYPT), the IACR area conferences (PKC, TCC, CHES, and FSE), and important security conferences such as IEEE Symposium on Security and Privacy and ACM Conference on Computer and Communications Security.

Collaboration with other French and European projects will continue to be done through communication with partners from research projects in which ENS is currently involved such as RISQ [19] and aSCEND [17].

3.2.3 FUAS

As a university FUAS main domain of competence is scientific research. The personnel involved in the FENTEC project for FUAS are professors or (post)-doctoral researchers doing research directly related to functional encryption. For those reasons, the two media FUAS will focus on are the following:

- The main contribution of FUAS towards the dissemination of FENTEC material will be the participation to peer-reviewed international scientific conferences, industrial conferences, workshops, fairs and professional meetings. This is partly conditioned by the production of papers of quality on functional encryption.
- The second medium of dissemination that FUAS will use are scientific papers. As FUAS research on functional encryption are commissioned by the FENTEC project, FUAS publications on the subject of functional encryption, or directly related to it, will try its best to promote the FENTEC project as well as tie the innovations presented in the paper to FENTEC use-cases and scenarios.

FUAS will teach functional encryption to students. In 2020, Prof. Dr. Gajek will teach the course Hot Topics in IT-Security which deals with the basics of functional encryptions, including identity, attribute and predicate encryption. FUAS will disseminate project results through private channels such as internal mailing list, as well as the ITSC group social media channels like Twitter and blogs. FUAS will also promote functional technology as a new solution opportunity for industry players. Of course, FUAS will be ready to exploit unexpected dissemination opportunities, such as new events, publication opportunities, or other media offering the possibility of disseminating the FENTEC project.

3.2.4 KUD

While KUD focus will remain on the exploitation of the outcomes of FENTEC, KUD is still open towards publishing results and will be actively participating in FENTEC cryptography research. This may lead to joint scientific publications with the other partners.

For internal communication, KUD has a “crypto guild”, which is a group of about 15 cryptographers that regularly meet and discuss on cryptography related topics. FENTEC is being regularly discussed and presented there.

For external communication, KUD will include and discuss FENTEC material on its research blog [27] and KUD will also promote FENTEC in appropriate marketing-related events, exhibitions or conferences, such as CARDIS or Black Hat. KUD will also continue to communicate on the FENTEC project through various online and offline marketing and communications activities, notably on its website in the “Research and Development” and “Industry alliances” sections. KUD might also set up a dedicated landing page for people requesting more info on the FENTEC project, and include FENTEC events or publications in Kudelski Security cybersecurity newsletter (sent internally and to cybersecurity professionals every day).

KUD will also continue its promotion activities on social media platforms such as Twitter and LinkedIn, as well as release one or more “Media alerts” regarding the project.

3.2.5 KU Leuven

For internal dissemination, KU Leuven will use departmental and sub-departamental meetings and mailing lists, e.g., COSIC [15], CiTiP [14], Data Protection and Privacy Group mailing lists as well as monthly and weekly internal meetings.

Dissemination towards the research community is done by publishing results in highly visible and relevant outlets, i.e., top journals and conferences in the field such as Data Privacy Law and European Data Protection Law Review, Computer Law & Security Review; Computers, Privacy and Data Protection Conference, IEEE Symposium on Security and Privacy, USENIX, ACM Conference on Computer and Communications Security, IACR flagship conferences (CHES, CRYPTO, EUROCRYPT, ASIACRYPT) or the Amsterdam Privacy Conference, among others. On the occasion of its 30th anniversary, CITIP has published a book entitled Security and Law, which includes a section on human rights and encryption.

COSIC is actively participating in the ongoing competition for Post-Quantum Cryptography, to which they have submitted four proposals for various algorithms (SABER, LUOV, Ramstake and LIMA). SABER and LUOV have been selected for the second round of the competition.

Collaboration with other European projects is done through communication with partners from European research projects on which KU Leuven was or is currently involved in such as WITDOM [24], CLARUS [20], BOSS [25], PDP4E [22].

3.2.6 UEDIN

UEDIN will continue to use internal communication channels to promote the FENTEC project and to communicate and disseminate its outcomes. The main channel for this purpose is UEDIN’s internal “cryptosec” mailing list that includes security and cryptography researchers in the university, the related weekly team meetings and the security-privacy mailing list that reaches out to hundreds of cyber security researchers in the general Scotland area. Beside this, UEDIN also uses its external communication channels, such as the Twitter account of the School of Informatics (@InfAtEd) to tweet or retweet FENTEC related work done by UEDIN and the other FENTEC partners.

As a leader of D4.4 “Annual Report on Functional Encryption Schemes with Richer Functionality” the main dissemination activity of UEDIN is to publish scientific papers in high impact scientific conferences. Especially the IACR conferences (such as CRYPTO, EUROCRYPT, TCC, ASIACRYPT, PKC) should be mentioned as relevant conferences in this area. Also, presentations at summer schools or workshops can be done to present UEDIN’s work.

Collaborations with researchers from related H2020 projects running concurrently at UEDIN will continue, these contain the PANORAMIX [21] and the PRIViLEDGE [23] projects. Beside this, UEDIN is also involved in the OXCHAIN [18] project funded by EPSRC. We continue to utilise the dissemination channels of the Blockchain Technology Laboratory at UEDIN and its industry partners (that include IOHK and Huawei) to disseminate results and engage with industry collaborators outside the FENTEC consortium that are interested in the project's outputs.

3.2.7 UH

UH is the leader of WP2 Dissemination, Communication, Standardisation and Exploitation.

UH will use internal communication channels to promote FENTEC and to communicate and disseminate its outcomes. Examples include the CS department's internal meetings and mailing lists. UH will use also the department's communication channels such as the Twitter account (@UnivHelsinkiCS) for (re)tweeting UH related work done in FENTEC.

The main dissemination activity of UH is to publish scientific papers in high impact scientific conferences and journals. Relevant conferences include IACR conferences (such as CHES, CRYPTO, EUROCRYPT, ASIACRYPT), IEEE S&P, ACM CCS, USENIX Security, etc. Relevant scientific journals include: IEEE Transactions on Computers, IEEE Transactions on VLSI Systems, Journal of Cryptographic Engineering, etc.

On the national (Finnish) level, UH will promote FENTEC in national seminars and workshops on information security and computer science. One example is the Annual Secure Systems Demo Day organized every June jointly by researchers of UH and Aalto University. Communication will be done also with Finnish research projects and within the community of Finnish information security experts.

3.2.8 Wallix

For WALLIX we have attended various technical conferences while promoting our DataPEPS product, including O'Reilly Velocity 2018, London, UK, Cyber Security X 2018, London, UK and DEVOXX 2018, Antwerp, Belgium. While the FENTEC project has not yet produced any software which we can demonstrate, we have discussed the goals of the project with many interested parties. Our goal for dissemination remains in contacting clients who may have an interest in our web analytics prototype or the associated technology.

The list of trade shows and industry journals we intend to target remains the same, in particular the ESOCC, the Forum International de la Securité and also Les Assises de la Securité.

As work progresses on the Web Analytics prototype we will have more information and hopefully a prototype which we can demonstrate to potential clients. We are also planning a paper on the prototype for a venue yet to be decided.

3.2.9 XLAB

With years of experience, XLAB's dissemination specialists and technology experts combine their expertise with data driven insights to draw up viable dissemination and communication strategies.

XLAB's content/design team works closely with the marketing/entrepreneurial team to deliver strong value and support the exploitation team, bridging the gap between research results and exploitation with a clearly defined set of activities.

XLAB will set up professional product websites (linked to XLAB website, 63,000 views/year, XLAB products page 945 pageviews/year), create newsletter and factsheets, and make social media appearances for technology transfer, better mapping and targeting stakeholders (e.g., Twitter - 511 followers, LinkedIn - 573 followers, Facebook - 503 followers).

XLAB will regularly attend international events (CSA CEE, CeBIT expo, ISC HPC, HiPEAC, DEFCON, Linux conferences, Euro-Par conference, CloudWATCH Summit), sponsor and participate national events (DragonHack, WebCamp Ljubljana, SecTalks Ljubljana, FRI USA Tour, JobFair, BSidesLjubljana), and organize workshops/hackatons for students together with the Faculty of Computer and Information Science (devops, continuous integration/deployment demonstration with open source/relevant technologies).

XLAB ensures all results are rendered openly available by using repositories for open source software (XLAB's GitHub, linked to X OPEN, 1,043 pageviews since launch December 2017).

XLAB will also utilize partner networks, liaison with related projects and relevant initiatives participation for its communication and dissemination.

In Y2, XLAB continued to develop two main FENTEC libraries (GoFE and CiFEr). Both libraries are publicly available on Github. Additionally, a few demonstrators have been published on Github which should make the adoption of functional encryption faster and easier.

4 Conclusions

This deliverable presented the dissemination activities and results obtained during Y2, the second project year 2019, and reflected them with the plans provided in D2.2 "Dissemination Plan" [9] and D2.3 "Annual Dissemination Report & Material Y1" [10]. The dissemination activities described in these deliverables have been active during Y2 and they have resulted in scientific publications as well as participations and presentations at scientific events. The efforts regarding standardization have been continued and were discussed in more detail in D2.11 "Preliminary Standardisation Report" [11]. The PAB of FENTEC was set up in Y1 and the second online PAB meeting was held in October 2019 (M22). To conclude, dissemination activities have progressed according to the plans from D2.2 [9].

Table 4 shows the KPIs and results for Y2. It can be observed that FENTEC was able to meet all KPIs that were set for Y2. In particular, FENTEC was able to publish 12 scientific articles in high-quality scientific venues, which is a good result. The presentations and participations in conferences are mostly related to presenting these results. During Y2, FENTEC was also able to achieve the standardization KPIs that have been set for the entire duration of the project. FENTEC has applied for a liaison to ISO (in Y1) and ETSI (in Y2). FENTEC also contacted NIST (in Y1), but a common ground for collaboration was not found. So, the KPI on standardization organizations contacted is met. FENTEC has reviewed standardization documents from both ISO (WG2 SD8) and ETSI (Guide to Identity Based Encryption), and thus, the document review KPI has also been met. The KPIs for standardization were planned to be achieved for the whole period of the project and if the liaison with ISO is accepted, FENTEC should be able to achieve them. In Y2, FENTEC organized the second PAB meeting.

KPI	Time	Threshold	Result
Scientific publications	Y2	4	12
Presentations in conferences	Y2	4	10
Participations in events	Y2	5	8
Standardization organization contacts	Y1-Y3	3	3
Liaison agreements	Y1-Y3	1	2
Standardization organization communication activities	Y1-Y3	3	3
Standardization document reviews	Y1-Y3	2	2
PAB meetings	Y2	1	1
PAB members present	Y2	6	3

Table 4: KPIs and results for Y2

To summarize, the dissemination outcomes during Y2 included:

- 12 scientific publications (11 published and 1 accepted);
- 8 other publications (mostly related to press releases); and

- 8 scientific events attended.

Additionally, FENTEC has continued discussions with relevant standardization bodies and held one online PAB conference. All KPIs for dissemination that were set in D2.2 [9] were achieved during Y2. Also standardization and PAB activities are progressing according to the plans and have achieved their KPIs.

The KPIs related to dissemination for Y3 are collected in Table 5. They were originally set in D2.2 [9], but they are repeated here in order to provide a clear picture of what FENTEC dissemination activities are expected to outcome during Y3.

KPI	Time	Threshold
Scientific publications	Y3	4
Presentations in conferences	Y3	5
Participations in events	Y3	5
Standardization organization contacts	Y1-Y3	3
Liaison agreements	Y1-Y3	1
Standardization organization communication activities	Y1-Y3	3
Standardization document reviews	Y1-Y3	2
PAB meetings	Y3	1
PAB members present	Y3	6

Table 5: KPIs for Y3

References

[1] Michel Abdalla, Fabrice Benhamouda, and Romain Gay. From single-input to multi-client inner-product functional encryption. In *Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8-12, 2019, Proceedings, Part III*, pages 552–582, 2019. (Pages 9, 10, and 13)

[2] Michel Abdalla, Fabrice Benhamouda, Markulf Kohlweiss, and Hendrik Waldner. Decentralizing inner-product functional encryption. In *Public-Key Cryptography — PKC 2019*, volume 11443 of *Lecture Notes in Computer Science*, pages 128–157. Springer, 2019. (Pages 9, 10, and 13)

[3] Manuel Barbosa, Dario Catalano, Azam Soleimanian, and Bogdan Warinschi. Efficient function-hiding functional encryption: From inner-products to orthogonality. In *Topics in Cryptology — CT-RSA 2019*, volume 11405 of *Lecture Notes in Computer Science*, pages 127–148. Springer, 2019. (Pages 9, 10, and 13)

[4] Ward Beullens, Jean-Charles Faugère, Eliane Koussa, Gilles Macario-Rat, Jacques Patarin, and Ludovic Perret. PKP-Based Signature Scheme. In *Progress in Cryptology - INDOCRYPT 2019*, Lecture Notes in Computer Science. Springer, 2019. To appear. (Pages 9 and 10)

[5] Ward Beullens and Hoeteck Wee. Obfuscating Simple Functionalities from Knowledge Assumptions. In Dongdai Lin and Kazue Sako, editors, *Public-Key Cryptography - PKC 2019, Proceedings, Part II*, volume 11443 of *Lecture Notes in Computer Science*, pages 254–283. Springer, 2019. (Pages 9, 10, and 13)

[6] Edouard Dufour-Sans and David Pointcheval. Unbounded inner-product functional encryption with succinct keys. In *Applied Cryptography and Network Security — ACNS 2019*, volume 11464 of *Lecture Notes in Computer Science*. Springer, 2019. (Pages 10 and 13)

[7] Danaja Fabcic. Protecting human rights through a global encryption provision. *Security and Law*, 2019. (Pages 9 and 10)

[8] FENTEC. D1.1 work plan Y1, 2018. (Page 16)

[9] FENTEC. D2.2 dissemination plan, 2018. (Pages 7, 9, 16, 22, and 23)

[10] FENTEC. D2.3 annual dissemination report & material Y1, 2018. (Pages 7 and 22)

[11] FENTEC. D2.3 preliminary standardisation report, 2019. (Pages 7 and 22)

[12] Romain Gay. *Public-Key Encryption, Revisited: Tight Security and Richer Functionalities.* PhD thesis, École normale supérieure Paris, 2019. (Pages 9 and 10)

[13] Angshuman Karmakar, Sujoy Sinha Roy, Frederik Vercauteren, and Ingrid Verbauwhede. Pushing the speed limit of constant-time discrete Gaussian sampling. A case study on the Falcon signature scheme. In *Design Automation Conference - DAC 2019*, pages 88:1–88:6. ACM, 2019. (Pages 9, 10, and 13)

[14] KU Leuven. Centre for IT & IP Law (CiTiP). https://www.law.kuleuven.be/citip, last retrieved on Nov. 1, 2018. (Page 19)

[15] KU Leuven. Computer Security and Industrial Cryptography (COSIC). http://www.esat.kuleuven.be/cosic/, last retrieved on Nov. 1, 2018. (Page 19)

[16] Tilen Marc, Miha Stopar, Jan Hartman, Manca Bizjak, and Jolanda Modic. Privacy-enhanced machine learning with functional encryption. In *Computer Security — ESORICS 2019*, volume 11735 of *Lecture Notes in Computer Science*, pages 3–21. Springer, 2019. (Pages 9, 10, and 14)

[17] Project. aSCEND. https://www.di.ens.fr/~wee/ascend/. (Page 18)

[18] Project. Oxchain. http://oxchain.uk. (Page 20)

[19] Project. RISQ. https://risq.fr/?page_id=31&lang=en. (Page 18)

[20] EU Project. CLARUS. http://www.clarussecure.eu/, last retrieved on Nov. 1, 2018. (Page 19)

[21] EU Project. Panoramix. https://panoramix-project.eu. (Page 20)

[22] EU Project. PDP4E. https://www.pdp4e-project.eu/, last retrieved on Nov. 1, 2018. (Page 19)

[23] EU Project. PRIViLEDGE. https://priviledge-project.eu/. (Page 20)

[24] EU Project. WITDOM. http://www.witdom.eu, last retrieved on Nov. 1, 2018. (Page 19)

[25] Research Project. BOSS. https://distrinet.cs.kuleuven.be/research/projects/BoSS, last retrieved on Nov. 1, 2018. (Page 19)

[26] Theo Ryffel, Edouard Dufour Sans, Romain Gay, Francis Bach, and David Pointcheval. Partially encrypted machine learning using functional encryption. *CoRR*, abs/1905.10214, 2019. (Pages 9, 10, and 14)

[27] Kudelski Security. Research Blog. https://research.kudelskisecurity.com/, last retrieved on Nov. 1, 2018. (Page 18)

[28] Miha Stopar, Manca Bizjak, Jolanda Modic, Jan Hartman, Anže Žitnik, and Tilen Marc. emmy — trust-enhancing authentication library. In *Trust Management XIII*, volume 563 of *IFIP Advances in Information and Communication Technology*, pages 133–146. Springer, 2019. (Pages 9, 10, and 14)