Disclaimer

Statement for open documents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780108. Any dissemination of results here presented reflects only the consortium view.

D2.3 Annual Dissemination Report & Material Y1

Document Identification			
Status	Final	**Due Date**	31/12/2018
Version	1.0	**Submission Date**	11/12/2018

Related WP	WP2	**Document Reference**	D2.3
Related Deliverable(s)	D1.1, D1.4, D2.1, D2.2, D2.4, D2.5, D2.8, D2.9. D2.10	**Dissemination Level(*)**	PU
Lead Participant	UH	**Lead Author**	Kimmo Järvinen (UH)
Contributors	All partners	**Reviewers**	Marco Lewandowsky (FUAS) Svetla Nikova (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
José Crespo Martin	ATOS
Francisco Gala	ATOS
Svetla Nikova	KU Leuven
Danaja Fabčič Povše	KU Leuven
Miha Stopar	XLAB
Yolan Romailler	KUD
Robert Bowers	KUD
Hendrik Waldner	UEDIN
Norman Scaife	WALLIX
Michel Abdalla	ENS
Clément Gentilucci	FUAS

Document History			
Version	Date	Change editors	Changes
0.1	16/10/2018	Kimmo Järvinen (UH)	ToC
0.2	01/11/2018	Kimmo Järvinen (UH)	Updated ToC, input from partners
0.3	29/11/2018	Kimmo Järvinen (UH)	New content and input from partners
0.4	30/11/2018	Kimmo Järvinen (UH)	The version for internal review
0.5	04/12/2018	Francisco Gala (ATOS)	Corrections
0.6	07/12/2018	Kimmo Järvinen (UH)	Final review version
1.0	11/12/2018	Kimmo Järvinen (UH)	Final version

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable Leader	Kimmo Järvinen (UH)	11/12/2018
Technical Manager	Michel Abdalla (ENS)	11/12/2018
Quality Manager	Diego Esteban (ATOS)	11/12/2018
Project Coordinator	Francisco Gala (ATOS)	11/12/2018

Table of Contents

List of Tables

List of Acronyms

Abbreviation / acronym	Description
ACM	Association for Computing Machinery
CS	Computer Science
EU	European Union
ESOCC	European Conference on Service-Oriented and Cloud Computing
ETSI	European Telecommunications Standard Institute
IACR	International Association for Cryptologic Research
ICT	Information and Communication Technology
IEEE	Institute of Electrical and Electronics Engineers
IFIP	International Federation for Information Processing
ISO	International Organization for Standardization
KPI	Key Performance Indicator
PAB	Project Advisory Board
WP	Work Package
Y1	Year 1 (2018)
Y2	Year 2 (2019)

Executive Summary

In this deliverable D2.3 “Annual Dissemination Report & Material Y1”, we present a summary of dissemination activities of FENTEC during the first project year (Y1) from January 2018 (M01) to December 2018 (M12). 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 D2.8 “Annual Communication Activities Report Y1”. In addition to scientific outcomes, this deliverable also presents overviews of standardization and PAB activities. We also update the dissemination plan of FENTEC for the second project year (Y2) from January 2019 (M13) to December 2019 (M24). The original dissemination plan was described in D2.2 “Dissemination Plan” submitted in June 2018 (M6).

To summarize, the dissemination outcomes during Y1 included:

- 7 scientific publications (5 published and 2 accepted);
- 12 press releases (2 in English and 10 in Spanish); and
- 9 events attended.

Additionally, FENTEC has initiated contacts with relevant standardization bodies and held one online PAB conference. All KPIs for dissemination that were set in D2.2 were achieved during Y1. Also standardization and PAB activities are progressing according to the plans.

1 Introduction

1.1 Purpose of the document

This deliverable D2.3 "Annual Dissemination Report & Material Y1" describes the dissemination activities and their outcomes for the first project year Y1, from January 2018 (M1) to December 2018 (M12). 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, but T2.4 and T2.5 are also shortly surveyed. The task T2.2 "Communication activities" will be discussed in detail in D2.8 "Annual Communication Activities Report Y1".

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 D2.8. 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 Y1. Further details about the PAB and the outcomes of the first PAB meeting will be provided in D2.13 "Project Advisory Board Workshops Report Y1". Standardization related issues will be more closely discussed in D2.11 "Preliminary Standardisation Report" to be submitted in M18.

D2.2 "Dissemination Plan" [7], submitted in June 2018 (M6), defined KPIs for dissemination, standardization, and PAB. The dissemination KPIs for Y1 are:

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

The standardization KPIs for the entire duration of the project 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 Y1 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 Y2 regarding the KPIs not met in Y1.

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 Y1.
- Section 3 presents the updated dissemination plan for Y2.
- Section 4 ends the deliverable with conclusions and studies how the project performed regarding the KPIs for Y1.

2 Dissemination activities and material

This section describes the dissemination activities and results during Y1. 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. In the end, Section 2.5 discusses liaison with other relevant research projects.

2.1 Publications

The main research outputs of FENTEC are scientific publications published in relevant scientific conferences and journals. During Y1, FENTEC produced the first 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 [7].

Table 1 collects the scientific publications produced by FENTEC that have been either published already or have been accepted to be published. It shows that the total number of scientific publications is seven. All of them have been (or are accepted to be) published in leading scientific venues in the fields of cryptology or cryptographic hardware. In particular, CRYPTO, EUROCRYPT and ASIACRYPT are the leading conferences in cryptology whereas CHES (and its journal TCHES) is the leading venue in cryptographic hardware and embedded systems.

The topics of the scientific publications are related either to new functional encryption schemes or relevant building blocks [1, 5, 3, 4, 2] or implementation techniques that are relevant also for functional encryption schemes [8, 24]. FENTEC was able to produce seven scientific publications during Y1 which can be considered as a good result for the first project year.

In addition to the scientific publications, FENTEC has published press releases in order to increase the awareness and visibility of the project. Two of the press releases were targeted for international audience and written in English, and a number of press releases were published in Spanish by Atos to raise attention in Spain. Details about the press releases 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 Y1, 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. In addition to scientific conferences, other

Authors, title, the name of the conference or journal	Status	Partner(s)
Jie Chen, Junqing Gong, Lucas Kowalczyk, and Hoeteck Wee: "Unbounded ABE via Bilinear Entropy Expansion, Revisited," **Advances in Cryptology — EUROCRYPT 2018** [3]	Published	ENS
Michel Abdalla, Dario Catalano, Dario Fiore, Romain Gay, and Bodgan Ursu: "Multi-Input Functional Encryption for Inner Products: Function-Hiding Realizations and Constructions without Pairings," **Advances in Cryptology —- CRYPTO 2018** [1]	Published	ENS
Jérémy Chotard, Edouard Dufour Sans, Romain Gay, Duong Hieu Phan, and David Pointcheval: "Decentralized Multi-Client Functional Encryption for Inner Product," **Advances in Cryptology — ASIACRYPT 2018** [5]	Published	ENS
Jie Chen, Junqing Gong, Hoeteck Wee: "Improved Inner-product Encryption with Adaptive Security and Full Attribute-hiding", **Advances in Cryptology —- ASIACRYPT 2018** [4]	Published	ENS
Angshuman Karmakar, Jose Maria Bermudo Mera, Sujoy Sinha Roy, and Ingrid Verbauwhede: "Saber on ARM. CCA-secure module lattice-based key encapsulation on ARM," **IACR Transactions in Cryptographic Hardware and Embedded Systems** 2018(3):243–266, 2018 [8]	Published	KU Leuven
Ward Beullens, Bart Preneel, and Alan Szepieniec: "Public Key Compression for Constrained Linear Signature Schemes," **Selected Areas in Cryptography — SAC 2018** [2]	To appear	KU Leuven
Sujoy Sinha Roy, Furkan Turan, Kimmo Järvinen, Frederik Vercauteren, and Ingrid Verbauwhede: "FPGA-based High-Performance Parallel Architecture for Homomorphic Computing on Encrypted Data", **IEEE International Symposium on High-Performance Computer Architecture — HPCA 25** [24]	To appear	KU Leuven, UH

Table 1: Scientific publications by FENTEC during Y1

Title, authors, and other publication details	Publication type	Partner(s)
FENTEC Project: Increasing Trustworthiness of ICT solutions developing Functional Encryption Systems [Atos Global Website]	Press release	ATOS
Un nuevo Proyecto permite compartir datos en redes no seguras (in Spanish) [IT User]	Press release	ATOS
Atos lidera un proyecto europeo que permitirá compartir datos de forma segura a través de redes no seguras (in Spanish) [El Candelero Tecnológico]	Press release	ATOS
Proyecto FENTEC: Compartir datos de forma segura a través de redes no seguras (in Spanish) [Redes Telecom]	Press release	ATOS
FENTEC, proyecto europeo que desarrollará nuevos sistemas de encriptación funcionales (in Spanish) [Conectronica]	Press release	ATOS
Atos lidera un proyecto europeo que permitirá compartir datos de forma segura a través de redes no seguras (in Spanish) [Digital Affaires]	Press release	ATOS
Atos lidera un proyecto para securizar los datos en redes no seguras (in Spanish) [Computing]	Press release	ATOS
En marcha el proyecto FENTEC para compartir datos de forma segura a través de redes no seguras (in Spanish) [Data Center Market]	Press release	ATOS
Atos lidera un proyecto europeo que permitirá compartir datos de forma segura a través de redes no seguras (in Spanish) [Cybersecurity News]	Press release	ATOS
Atos lidera un proyecto europeo que permitirá compartir datos de forma segura (in Spanish) [Big Data Magazine]	Press release	ATOS
Proyecto FENTEC: compartir datos de forma segura a través de redes no seguras (in Spanish) [Telemática y Ciberseguridad]	Press release	ATOS
Media Alert about FENTEC [Kudelski News]	Press release	KUD

Table 2: Other publications by FENTEC during Y1

Name of the event	Location and date	Partner(s)
The 1st Cyberwatching.eu Concertation Meeting [www]	Brussels, Belgium April 26, 2018	ATOS
The 25th Conference on Selected Areas in Cryptography (SAC 2018) [www]	Calgary, AB, Canada Aug. 13–14, 2018	KU Leuven
IACR 38th Annual International Cryptology Conference (CRYPTO 2018) [www]	Santa Barbara, CA, USA Aug. 19-–23, 2018	ENS
IFIP Summer School on Privacy and Identity Management [www]	Vienna, Austria Aug. 20–24, 2018	XLAB
IACR Conference on Cryptographic Hardware and Embedded Systems (CHES 2018) [www]	Amsterdam, the Netherlands Sept. 9–12, 2018	KU Leuven UH
Black Alps 2018 [www]	Yverdon, Switzerland Nov. 8–9, 2018	KUD
The 17th Smart Card Research and Advanced Application Conference (CARDIS 2018) [www]	Montpellier, France Nov. 12–14, 2018	KUD
Black Hat Europe 2018 [www]	London, United Kingdom Dec. 3–6, 2018	KUD
IACR 24th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2018) [www]	Brisbane, Australia Dec. 2–6, 2018	ENS KU Leuven

Table 3: Conferences and other events where FENTEC participated during Y1

events such as European networking meetings, summer schools, and more industry-focused security events were in the scope of FENTEC. The events, in which FENTEC members participated, are collected in Table 3 and discussed more closely below.

2.2.1 Cyberwatching

Alberto Crespo from Atos presented FENTEC at the Cyberwatching.eu Concertation Meeting that took place in Brussels on April 26th 2018. He presented the FENTEC project within breakout session 2: "Foundational technical methods and risk management for trustworthy systems", presenting an overview of the project as well as its next steps and collaboration opportunities. He actively participated in the roundtable discussion that followed to identify Top 5 R&I Challenges, Top 5 Cross cutting themes, Top 5 New collaboration opportunities and new ideas[1]. Cyberwatching included a web page with information about FENTEC. The project was also further presented to other partners as part of informal networking talks in event breaks, where valuable contacts with other projects were made and FENTEC Press Release was also made available to participants.

The event counted with strong presence of EU representatives, including FENTEC's Project Officer, Dr. Nineta Polemi and represented a major clustering opportunity to exchange ideas

[1] see https://www.cyberwatching.eu/sites/default/files/Concertation_Meeting_Breakout_2_Results.pdf

on common themes in cybersecurity and privacy ecosystem and to gain awareness about major initiatives (e.g. Cybersecurity Atlas).

2.2.2 SAC 2018

SAC is an annual conference in selected areas of cryptography, which always takes place in Canada. This year KU Leuven was present at the conference by two members of the FENTEC team - Svetla Nikova and Ward Beullens. Ward Beullens presented his FENTEC related paper [2]. Svetla Nikova was a member of the program committee.

2.2.3 CRYPTO 2018

CRYPTO is one of the three IACR general conferences and is always held in Santa Barbara, California, during the month of August. Four members of ENS were present at the conference: Miche Abdalla, Hoeteck Wee, David Pointcheval, and Romain Gay. The paper on multi-input functional inner-product encryption [1] was also presented at the conference.

2.2.4 IFIP Summer School

XLAB attended IFIP Summer School in Vienna and presented FENTEC Golang libraries. In particular, the presentation showed how machine learning classification can be done over encrypted data using FENTEC Golang library GoFe and Python/TensorFlow scripts.

2.2.5 CHES 2018

CHES 2018 was held in Amsterdam in September 2018. CHES is the leading venue in cryptographic hardware. Angshuman Kamakar from KU Leuven gave a presentation related to a FENTEC publication published in TCHES [8], the journal of the CHES conference. Participants from KU Leuven and UH had discussions about FENTEC and made plans on how to proceed with the work in WP5 of the project. Kimmo Järvinen from UH was a member of the program committee of CHES 2018.

2.2.6 Black Alps 2018

KUD attended Black Alps, in Switzerland, and could distribute the FENTEC flyers to the cryptographers attending the conference, and discuss possible collaboration on the topic with the HEIG-VD, the School of Management and Engineering Vaud.

2.2.7 CARDIS 2018

KUD attended CARDIS 2018 and FENTEC was presented in the opening talk of the last day of the conference by Brecht Wyseur in his invited talk titled “Challenges in Securing Industrial IoT and Critical Infrastructure”.

2.2.8 Black Hat Europe 2018

KUD attended Black Hat Europe 2018 where FENTEC was discussed with interested parties and leaflets were distributed during different meetings.

2.2.9 ASIACRYPT 2018

ASIACRYPT is one of the three IACR general conferences and takes place at a different country in Asia and Oceania around the beginning of December. Two members of ENS were present at the conference: David Pointcheval and Romain Gay. The papers on decentralized multi-client functional encryption [5] and on inner-product predicate encryption [4] co-authored by members of our team were also presented at the conference.

2.3 Standardization

During Y1 FENTEC has contacted two standardization bodies: ISO and ETSI. FENTEC applied for a liaison to ISO/IEC SC27 and their decision has not been made yet. FENTEC had initial conversations with ETSI during the Security week event in Sofia Antipolis in June 2018, where the Standardization task leader Svetla Nikova from KU Leuven was invited as a panelist. The industrial partner KUD in FENTEC is a member of ETSI. FENTEC has been invited to present the project and to discuss further opportunities for collaboration at the next meeting of ETSI in January 2019. A representative from KUD will attend the meeting.

2.4 Project advisory board (PAB)

The first PAB meeting took place online on November 26, 2018, during which the FENTEC partners presented a summary of the work performed during Y1 and the plans for the following years.

The PAB members present at the call were:

- Dr. Sven Bauer (Giesecke & Devrient, Germany)
- Prof. Sergey Gorbunov (University of Waterloo, Canada)
- Dr. Vadim Lyubashevsky (IBM Zurich, Switzerland)

In addition, additional feedback was obtained via email and individual calls with the remaining members of the PAB

- Dr. Antonio Kung (Trialog, France)
- Dr. Jesus Luna (Bosch and Technische Universität of Darmstadt, Germany)
- Dr. Ventzislav Nikov (NXP Semiconductors, Belgium)
- Dr. Claire Vishik (Intel Corporation, UK)

D2.13 Project Advisory Board Workshop Reports Y1 contains more details on the PAB, including a short CV of the members and the minutes of the Y1 online meeting.

2.5 Liaison with other research projects

In Y1, FENTEC has been in touch with the other three H2020 projects that were funded by the call H2020-DS-2016-2017: PRIViLEDGE [19], FutureTPM [16] and PROMETHEUS [20].

In May 2018, FENTEC prepared an application for the ICT 2018 event and took this opportunity to get in touch with these other projects in order to join forces. Unfortunately, FutureTPM did do not want to join and PROMETHEUS was still in the process of being set up.

On the other hand, PRIViLEDGE was very cooperative and, in the end, two joint applications were submitted. FENTEC applied for a networking session to be shared with PRIViLEDGE, and PRIViLEDGE applied for a booth to be shared with FENTEC. Unfortunately, both applications for the ICT were rejected.

In Y2, FENTEC will keep in touch with these projects and explore new cooperation opportunities such as joint workshops, conference calls to share results, etc.

3 Dissemination plans for the next year

This section presents an updated dissemination plan for Y2. 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 [7] are still valid and exercised also for Y2 of the project. In the following, we survey certain key aspects, but the reader is referred to D2.2 [7] 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" [6] 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 [7], respectively, and they are still perfectly valid also for Y2.

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 the same trend will be continued during Y2.

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

Atos is the Project and Innovation Manager and coordinates the communication tasks within FENTEC project, making important efforts in WP2. In this role, Atos has been acting proactively in every dissemination opportunities through online and offline channels.

For Y2, Atos will still make use of internal and external channels to spread FENTEC results and achievements through several ICT audiences. As the partner responsible for communications, Atos will closely work with the dissemination team in order to make scientific content comprehensible for everyone. Thus, the audience reached will be wider.

Atos corporate communication structures will continue to be used as strategic tools for results' communication to targeted audiences:

- Marketing and communication department: For official press releases and news
- Internal Communities: ZEN, Atos Thought Leadership Blog, Website, etc
- Atos Scientific Community
- Internal Magazines: Axia Corporate Magazine, Atos Thought Leadership Blog

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 Y1, 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 ECRYPT-NET [15], RISQ [13], and aSCEND [11].

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 paper 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 summer semester 2019, Prof. Dr. Gajek will read 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 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 [23] 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 setup 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 [10], CiTiP [9], 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.

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).

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 [21], CLARUS [14], BOSS [22], PDP4E [18].

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 [17] and the PRIViLEDGE [19] projects. Beside this, UEDIN is also involved in the OXCHAIN [12] 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 and 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 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 Y1, XLAB created FENTEC account on Github where all FENTEC libraries will be released (currently Golang library and Python machine learning demostrator). In Y2, when other FEN-

TEC libraries will be added, XLAB will try to reach as much audience as possible and regularly communicate about added features and extensions to build a community and raise the awareness of functional encryption technologies.

4 Conclusions

This deliverable presented the dissemination activities and results obtained during Y1, the first project year 2018, and reflected them with the plans provided in D2.2 "Dissemination Plan" [7]. The dissemination activities have been initiated and they have resulted in the first outcomes in the form of scientific publications and as participations and presentations at scientific events. The efforts regarding standardization have also began. The PAB of FENTEC has been set up and the first online PAB meeting was held in November 2018 (M11). To conclude, dissemination activities have progressed according to the plans from D2.2 [7].

Comparing the KPIs set in D2.2 [7] and listed in Section 1 with the results decribed in Section 2 reveals that almost all KPIs were met and some even significantly exceeded. A summary is provided in Table 4. The three dissemination related KPIs were all significantly exceeded. E.g., the threshold for scientific publications, which was arguably the most important metric, was two publications, but FENTEC resulted in 7 scientific publications during Y1 (5 published and 2 accepted). FENTEC has applied for a liaison to ISO and contacted ETSI to discuss possible cooperation. FENTEC also contacted NIST, but a common ground for collaboration was not found. So, the KPI on standardization organizations contacted is met. FENTEC has not reviewed standardization documents yet since the liaison should be accepted by ISO first. 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. Because FENTEC organized the first PAB meeting (online on Nov. 26, 2018) the first PAB KPI was successfully met. Unfortunately, only three out of seven PAB members were able to participate the meeting and, consequently, the second PAB KPI was not met (6 members should have attended). However, the material presented in the meeting was distributed to the other PAB members, which enabled them to give feedback despite not attending the actual PAB meeting.

KPI	Time	Threshold	Result
Scientific publications	Y1	2	7
Presentations in conferences	Y1	3	8
Participations in events	Y1	4	9
Standardization organization contacts	Y1-Y3	3	3
Liaison agreements	Y1-Y3	1	0
Standardization organization communication activities	Y1-Y3	3	3
Standardization document reviews	Y1-Y3	2	0
PAB meetings	Y1	1	1
PAB members present	Y1	6	3

Table 4: KPIs and results for Y1

To summarize, the dissemination outcomes during Y1 included:

- 7 scientific publications (5 published and 2 accepted);

- 12 press releases (2 in English and 10 in Spanish); and
- 9 events attended.

Additionally, FENTEC has initiated contacts with relevant standardization bodies and held one online PAB conference. All KPIs for dissemination that were set in D2.2 [7] were achieved during Y1. Also standardization and PAB activities are progressing according to the plans and achieved the most important KPIs.

The KPIs related to dissemination for Y2 are collected in Table 5. They were originally set in D2.2 [7], but they are repeated here in order to provide a clear picture of what FENTEC dissemination activities are expected to outcome during Y2. As the only specific measure for improving performance regarding KPIs, we recommend that the next year's PAB meeting should be planned and the date fixed earlier than in Y1 so that more PAB members could join the meeting. The performance regarding other KPIs was excellent and FENTEC aims to maintain the same performance level or even exceed it in Y2.

KPI	Time	Threshold
Scientific publications	Y2	4
Presentations in conferences	Y2	4
Participations in events	Y2	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	Y2	1
PAB members present	Y2	6

Table 5: KPIs for Y2

References

[1] Michel Abdalla, Dario Catalano, Dario Fiore, Romain Gay, and Bogdan Ursu. Multi-input functional encryption for inner products: Function-hiding realizations and constructions without pairings. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology — CRYPTO 2018*, volume 10991 of *Lecture Notes in Computer Science*, pages 597–627. Springer, 2018. (Pages 8, 9, and 12)

[2] Ward Beullens, Bart Preneel, and Alan Szepieniec. Public key compression for constrained linear signature schemes. In *Selected Areas in Cryptography — SAC 2018*, Lecture Notes in Computer Science. Springer, 2018. to appear. (Pages 8, 9, and 12)

[3] Jie Chen, Junqing Gong, Lucas Kowalczyk, and Hoeteck Wee. Unbounded ABE via bilinear entropy expansion, revisited. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology — EUROCRYPT 2018*, volume 10820 of *Lecture Notes in Computer Science*, pages 503–534. Springer, 2018. (Pages 8 and 9)

[4] Jie Chen, Junqing Gong, and Hoeteck Wee. Improved inner-product encryption with adaptive security and full attribute-hiding. In Steven Galbraith and Thomas Peyrin, editors, *Advances in Cryptology — ASIACRYPT 2018*, volume 11273 of *Lecture Notes in Computer Science*, pages 673–702. Springer, 2018. (Pages 8, 9, and 13)

[5] Jérémy Chotard, Edouard Dufour Sans, Romain Gay, Duong Hieu Phan, and David Pointcheval. Decentralized multi-client functional encryption for inner product. In Steven Galbraith and Thomas Peyrin, editors, *Advances in Cryptology — ASIACRYPT 2018*, volume 11273 of *Lecture Notes in Computer Science*, pages 703–732. Springer, 2018. (Pages 8, 9, and 13)

[6] FENTEC. D1.1 work plan y1, 2018. (Page 15)

[7] FENTEC. D2.2 dissemination plan, 2018. (Pages 6, 8, 15, 21, and 22)

[8] Angshuman Karmakar, Jose Maria Bermudo Mera, Sujoy Sinha Roy, and Ingrid Verbauwhede. Saber on ARM: CCA-secure module lattice-based key encapsulation on ARM. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2018(3):243–266, August 2018. (Pages 8, 9, and 12)

[9] KU Leuven. Centre for IT & IP Law (CiTiP). https://www.law.kuleuven.be/citip, last retrieved on Nov. 1, 2018. (Page 17)

[10] KU Leuven. Computer Security and Industrial Cryptography (COSIC). http://www.esat.kuleuven.be/cosic/, last retrieved on Nov. 1, 2018. (Page 17)

[11] Project. aSCEND. https://www.di.ens.fr/~wee/ascend/. (Page 16)

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

[13] Project. RISQ. https://risq.fr/?page_id=31&lang=en. (Page 16)

[14] EU Project. CLARUS. http://www.clarussecure.eu/, last retrieved on Nov. 1, 2018. (Page 18)

[15] EU Project. ECRYPT. http://www.ecrypt.eu.org/net/. (Page 16)

[16] EU Project. FutureTPM. https://futuretpm.eu/. (Page 14)

[17] EU Project. Panoramix. https://panoramix-project.eu. (Page 18)

[18] EU Project. PDP4E. https://www.pdp4e-project.eu/, last retrieved on Nov. 1, 2018. (Page 18)

[19] EU Project. PRIViLEDGE. https://priviledge-project.eu/. (Pages 14 and 18)

[20] EU Project. PROMETHEUS. https://cordis.europa.eu/project/rcn/213162_en.html. (Page 14)

[21] EU Project. WITDOM. http://www.witdom.eu, last retrieved on Nov. 1, 2018. (Page 18)

[22] Research Project. BOSS. https://distrinet.cs.kuleuven.be/research/projects/BoSS, last retrieved on Nov. 1, 2018. (Page 18)

[23] Kudelski Security. Research Blog. https://research.kudelskisecurity.com/, last retrieved on Nov. 1, 2018. (Page 17)

[24] Sujoy Sinha Roy, Furkan Turan, Kimmo Järvinen, Frederik Vercauteren, and Ingrid Verbauwhede. FPGA-based high-performance parallel architecture for homomorphic computing on encrypted data. In *IEEE International Symposium on High-Performance Computer Architecture — HPCA 25*. IEEE, 2019. to appear. (Pages 8 and 9)