



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.

Content

1. Project Overview
2. Achievements so far
3. Publications
4. Next Steps
5. Contact and Social Media

Functional **EN**ryption **TEC**nologies, FENTEC for short, offers a new paradigm to overcome the all-or-nothing limitations of classical encryption.

Functional Encryption (FE) deciphers a function over the message plaintext and makes it feasible to process encrypted data (e.g. on the Internet) and obtain a partial view of the message plaintext.

This extra flexibility over classical encryption is a powerful enabler for many emerging security technologies

FENTEC's mission is to make Functional Encryption readily available for wide-range applications, integrating the new paradigm into ICT technologies as naturally as classical encryption

Objectives of the project

Implement a unified **cryptographic API** of Functional Encryption systems

Validate and **demonstrate** FENTEC technologies and **solutions**



Design **functional encryption systems** with varying functional, security, **hardware** and **software** requirements

Use-Cases



Privacy-preserving and auditable Digital Currency



Data Collection and Local Decision Making



Privacy-Preserving Statistical Analysis

2018 is ending and FENTEC is wrapping up the first year of the project with already promising results.

It has been long since the Project kicked off in Madrid last January and the early days in which all the foundations were set. Now the Year-1 work plan is almost completed and the detailed schedule for the second years is currently being prepared.

A substantial amount of work was achieved in these twelve months, most remarkably:

- Back in February 2018 the project was officially presented to the general public via social media and the project webpage (www.fentec.eu).
- By early summer, the first technical output was released and the core FE requirements and metrics were defined .
- In September 2018 the first detailed description of the three use cases came along. Also, the Security and Trust models were released and, most importantly, the first work on the FE that would be used in the prototypes was submitted.
- Along this first year, FENTEC has also been building external links such as the Project Advisory Board (PAB) and standardisation bodies (ISO, ETSI)

FENTEC has participated in 13 Events and conferences in 9 countries

During 2018, 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 and delivered speeches about the work done in FENTEC. In addition to the scientific conferences, FENTEC Consortium also attended other events such as European networking meetings, summer schools, and industry-focused security event.






FENTEC Plenary Meeting, 24th October, Helsinki.

 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.

Miguel Ángel Mateo (Atos). FENTEC Plenary Meeting, Helsinki. 24 October 2018

 Click on the content to read and download papers

1

CCA-secure module lattice-based key encapsulation on ARM | [TCHES 2018](#)

Authors: Angshuman Karmakar, Jose Maria Bermudo Mera, Sujoy Sinha Roy and Ingrid Verbauwhede

2

Improved Inner-product Encryption with Adaptive Security and Full Attribute-hiding | [ASIACRYPT 2018](#)

Authors: Jie Chen, Junqing Gong and Hoeteck Wee

3

Decentralized Multi-Client Functional Encryption for Inner Product | [ASIACRYPT 2018](#)

Authors: Jérémy Chotard, Edouard Dufour Sans, Romain Gay, Duong Hieu Phan and David Pointcheval

4

Multi-Input Functional Encryption for Inner Products: Function-Hiding Realizations and Constructions without Pairings | [CRYPTO 2018](#)

Authors: Michel Abdalla, Dario Catalano, Dario Fiore, Romain Gay and Bodgan Ursu

5

Unbounded ABE via Bilinear Entropy Expansion, Revisted | [EUROCRYPT 2018](#)

Authors: Jie Chen, Junqing Gong, Lucas Kowalczyk and Hoeteck Wee

6

Public Key Compression for Constrained Linear Signature Schemes | [SAC 2018](#)

Authors: Ward Beullens and Bart Preneel and Alan Szepieniec

Visit fentec.eu and download
FENTEC latest Papers

We are now in December 2018 and the Consortium is hectically preparing a quite substantial delivery before the new year:

- The technical requirements will be completed with a set of legal and ethical requirements. FENTEC will continuously manage the potential risk of misusing our results!
- The first report on the implementation work done so far will be released. Up to date, FENTEC has implemented 4 schemes in 3 different languages, all available in the Project's GitLab.
- Additional developments on FE will be submitted, one on expressive FE and another report on the ground-breaking field of quantum-safe FE

All in all, the first project year has been a really busy year and the Consortium is looking forward to publishing all these results before the (well deserved!) holidays.

FENTEC will start the new year with a quick visit to Brussels to present the work done so far. The Consortium hopes to return with a positive feedback and also with good ideas on how to keep improving our results.

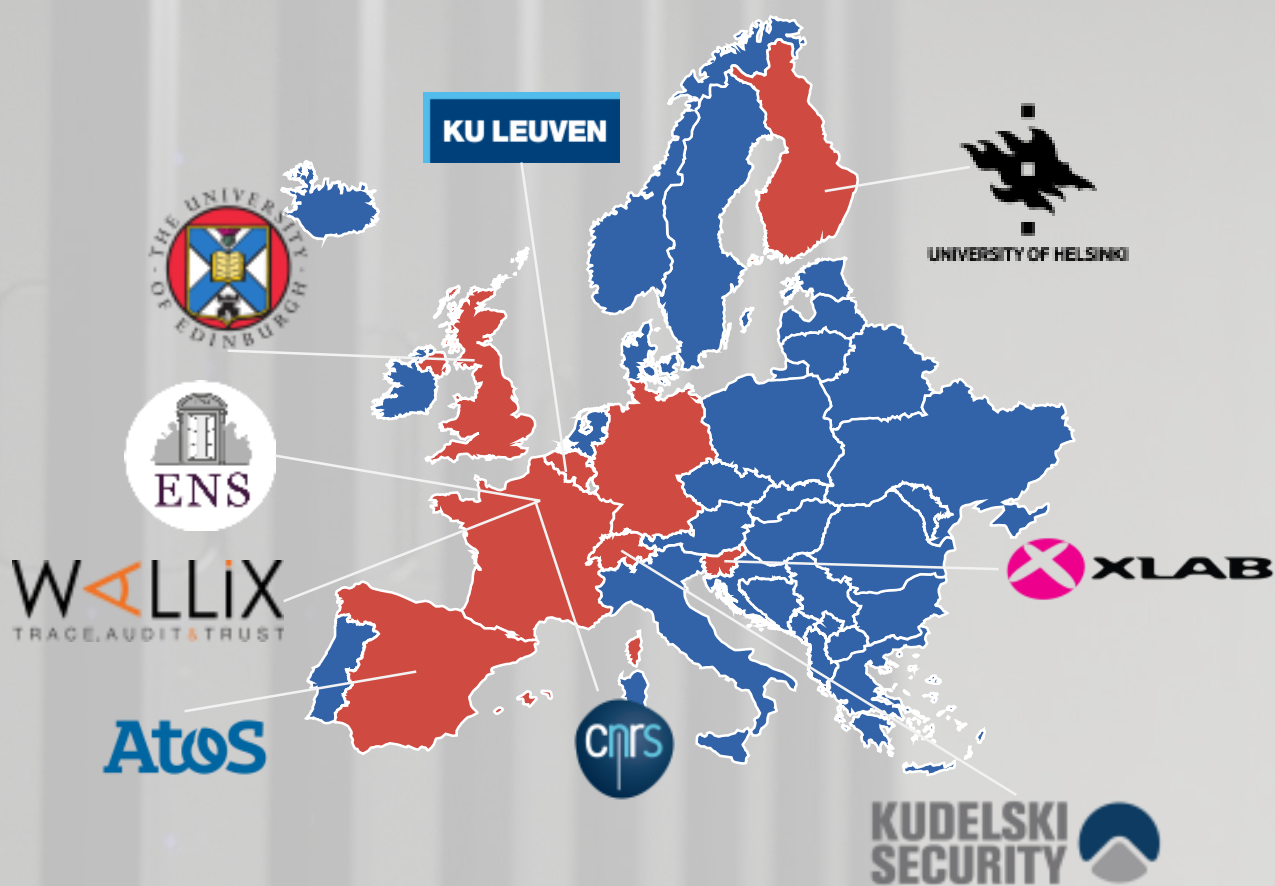
On top of that, more things are about to happen in the coming year, such as:

- More development of the FE algorithms is expected, with three reports due in 2019. The work on application-specific FE will be released by April, and toward the end of the year the other two reports on expressive FE and quantum-safe FE.

***Looking forward
to seeing FE in
action!***

- From May to September four reports on hardware (HW) support will present the work done up to that date. These tasks are already ongoing and by mid-2019 the first results on HW optimised/assisted/operated FE will be finished.
- The implementation of new FE schemes will carry on and a second report will be released in August 2019. Also beginning with the new year, the work on security verification will commence. In the second half of the year the optimization efforts will also launch.
- Lastly, the highly anticipated first version of the three prototypes will be ready by late-autumn 2019.

ARE YOU INTERESTED IN **FUNCTIONAL** **ENCRYPTION?**



www.fentec.eu



FENTEC Project



@FENTEC_project



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.