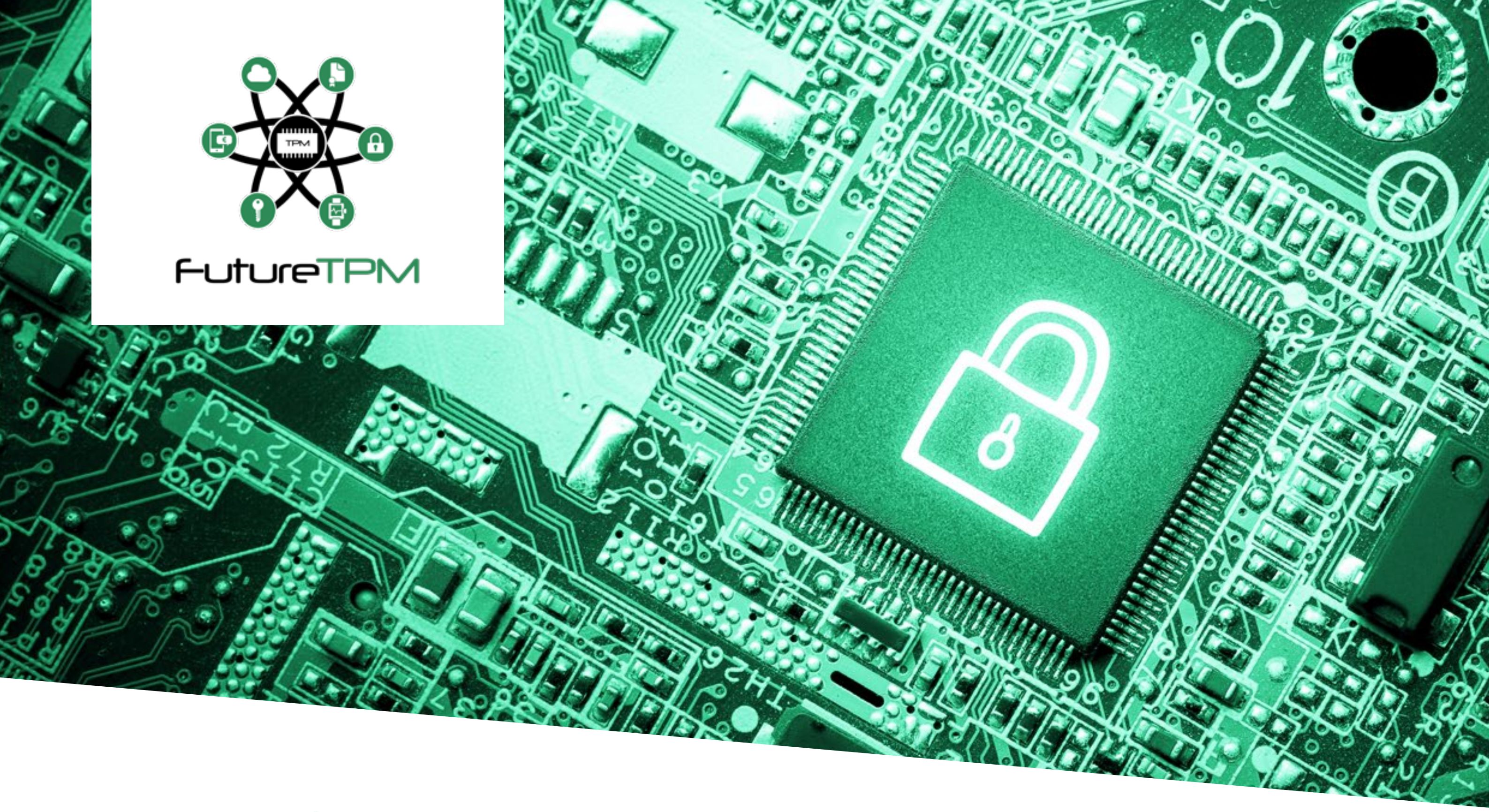


Newsletter / November 2018 - Issue 3

A Year of Progress

Project status update from Liqun Chen

Professor Liqun Chen
Technical Lead, FutureTPM
University of Surrey
liqun.chen@surrey.ac.uk

More than 10 months of the FutureTPM project passed. Therefore, we are able to report you the project's progress.

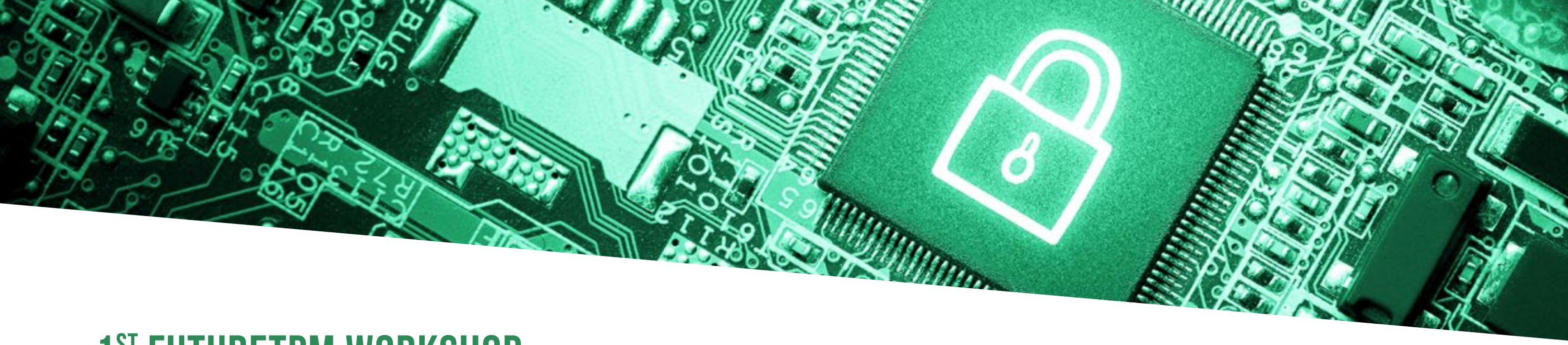
During this period, we have successfully completed the first work package, which defines the security and privacy requirements of the FutureTPM framework and the envisioned use cases. All the technical tasks have been completed and the deliverables of this work package have been submitted to the EU and have been published on the project website (futuretpm.eu).

The first three **project milestones** have been successfully achieved, namely:

- Availability of the FutureTPM Reference Architecture
- Availability of the technical, security and privacy requirements, to be met by the FutureTPM framework and the use cases
- Investigation of a wide set of QR cryptographic primitives, i.e. symmetric, asymmetric and privacy-preserving, so as to select the best ones for implementation in the various TPM environments (hardware-, software- and virtual-). This will also allow further investigation for the design of new QR crypto primitives especially for enhanced privacy preservation.

The project has been working in parallel on all the three core technical work packages: quantum-resistant cryptographic algorithms for a TPM (WP2); security modelling and analysis (WP3); and run-time risk assessment and vulnerability analysis (WP4). Work on the implementation and demonstration work packages will begin soon.

Table of contents



1ST FUTURETPM WORKSHOP

Check out the conference aftermovie on Vimeo

The 1st FutureTPM Workshop on Quantum-Resistant Crypto Algorithms was held in Lisbon on the 19th of October. The workshop's goal was to foster collaboration between different key players in the quantum-safe cryptography and trusted computing communities and others involved in similar projects.

The event was attended by more than 60 people both from the industry and academia. In addition to FutureTPM's partners, key organisations, such as TCG and NIST, and industry partners, such as HP Labs and Tales UK participated in the event as well.

The workshop was organised in four sessions and a following panel discussion.

The **first session** included three talks. The first talk presented an overview of the FutureTPM project to the audience. The second talk, given by **Dr Steve Hanna (Co-Chair of Embedded Systems Work Group at TCG)**, presented the future of Trusted Computing and TCG vision. In the third talk, **Dr Lily Chen (NIST)** presented the NIST vision for the future of post-quantum computing and related standardization activities.

The **second session** was dedicated to the use of trusted computing towards enhancing the security and privacy of real-world devices and applications. This session also showcased the FutureTPM use cases along with the view of TPM applications presented by **Dr Carey Huscroft (HP Labs)** and **Dr Adrian Waller (Tales UK)**.

The **third session** was dedicated to on-going EU projects addressing similar topics, such as **PQCrypto, SAFEcrypto, PROMETHEUS,** and was followed by a discussion on how to foster better collaboration between all these EU initiatives and other ongoing national projects.

The **last session** was dedicated to Quantum-Resistant TSS Implementation. Prior to that, a panel discussion, moderated by **Prof. Liqun Chen** took place. There, the participants addressed the challenges that TSS quantum-resistant implementations will face in the mid-term, and provided suggestions for FutureTPM use cases implementation.

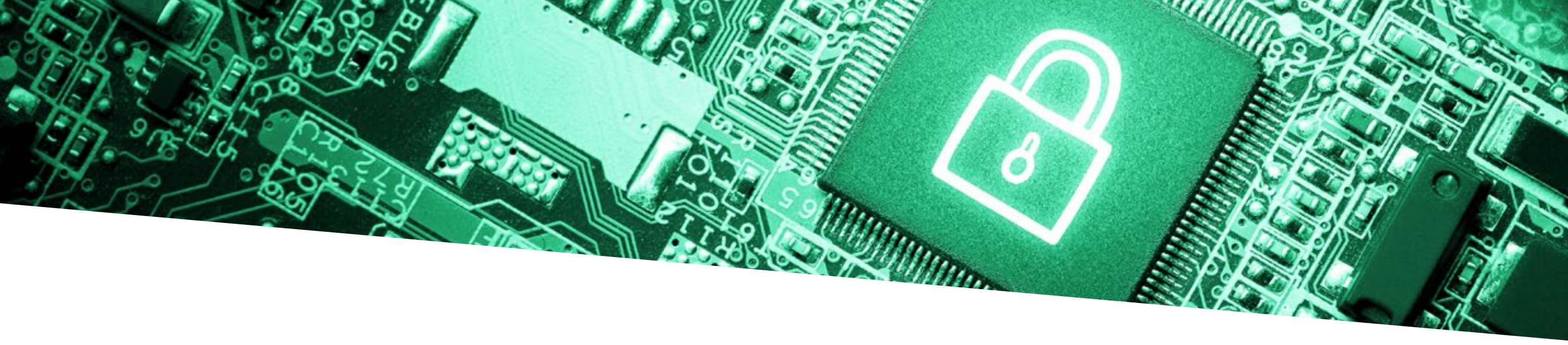
The FutureTPM consortium is very happy to have received such an enthusiast support from the community, and will take into account all feedback, recommendations and suggestions received during the event to improve the outcomes of the project.

> ***"I think this project will help with tackling the issues and come up with new solutions that will be very important for the industry in the future."***
>
> *Christian Gehrmann (Advisory Board Member)*

Check out another interviews from the FutureTPM consortium.

Thanassis Giannetsos (Technical Lead)

Liqun Chen (Technical Lead)



TECHNICAL AND 1ST ADVISORY BOARD MEETING IN LISBON

On the 18th of October, the FutureTPM consortium invited the Advisory Board members of the project to the first Advisory Board meeting in Lisbon, Portugal. The day before, on the 17th of October, an internal technical meeting took place. Both events were hosted by project partner INESC-ID.

The 17th of October was dedicated to the internal technical meeting which started with a summary of outputs and deliverables of WP1 that can be found on **futuretpm.eu**. WP1 "Requirements and Characterisation of the FutureTPM Framework" already ended in M09 (September) of the project. During the dedicated WP3 slot, partner SURREY led the discussion on TPM security modelling.

In the afternoon, a discussion on the QR algorithms to be selected for implementation per TPM environment, led by WP2 (WP-lead IBM) took place.

At the end of the day, the plan and open to-dos for Deliverable "Threat Modelling & Risk Assessment Methodology" were defined and the risk assessment tools to be employed and the vulnerability analysis of the TSS were discussed.

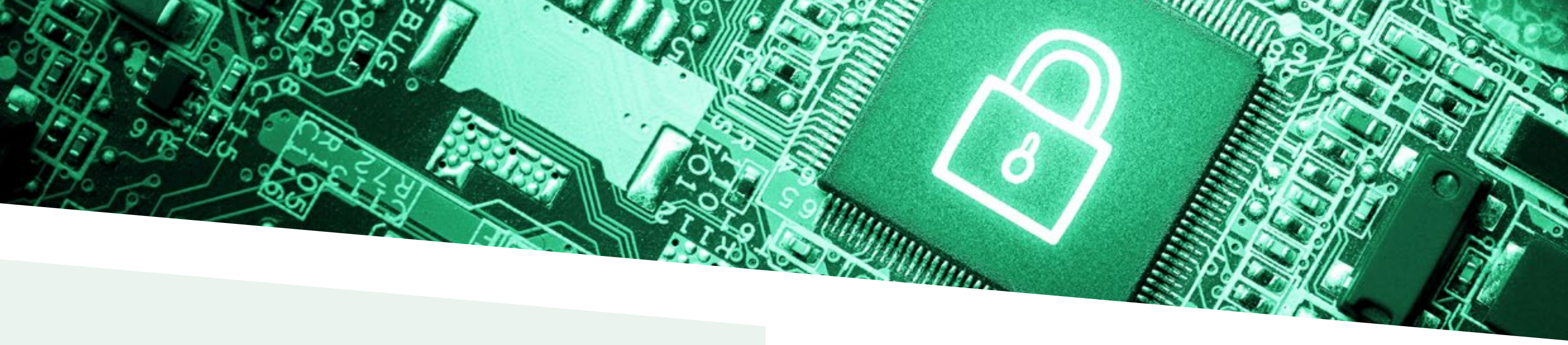
At the morning of day 2, before project partner IFAT opened the discussion on WP5 "QR TPM Implementation, Performance Evaluation AND Testing", a short slot for administrative issues was planned. In WP5, the focus of work for some partners were defined and some important decisions on how to proceed were made.

The afternoon of the second day was dedicated to the Advisory Board meeting. After a short round of introduction, Liqun Chen and Thanassis Giannetsos (University of Surrey), the technical leaders of the FutureTPM project, gave a short introduction to FutureTPM, including a technical project overview and the roadmap of the FutureTPM project.

After this short introduction, the leaders of the running (and finished) WPs presented the actual status of their WPs and the work already carried out. Fruitful discussions on the work done and the roadmap for the remaining project, which will be beneficial for the futuer project progress took place.

The FutureTPM team received valuable feedback and comments from the three Advisory Board members (Carey Huscroft – HP Labs, Christian Gehrmann - Gehrmann Trusted-ICT AB, Adrian Waller- Thales UK) to different aspects.

The feedback from the Advisory Board members was very positive and constructive. Overall, they were impressed and positively satisfied with the current project status.



SUBMITTED DELIVERABLES

Public RTD Deliverables published on FutureTPM

FutureTPM Reference Architecture

This deliverable provides the specification of the FutureTPM reference architecture, the functional components and interfaces between them. It also provides an analysis and point of reference for the FutureTPM in relation to the reference scenarios, including an analysis of the TPM commands to be used and updated, all relevant classical protocols and the use cases themselves.

Security Risks in QR Deployments

This deliverable includes documentation of the security problems and risks that the classical protocols utilized in the three use cases might face in the presence of quantum adversaries.

First Report on New QR Cryptographic Primitives

In this deliverable the editors began the analysis of quantum-resistant cryptographic primitives in respect to their use in FutureTPM. The final goal was to identify suitable algorithms for adoption in the FutureTPM specification.

First Report on Security Models for the TPM

In this report, the editors reviewed the FutureTPM requirements and identified effects on design and modelling targets and challenges. The editors then reviewed the state of the art in threat and security modelling, in general and as applied to the TPM and other similar TEEs.

UPCOMING PUBLIC DELIVERABLES

Public RTD Deliverables published on FutureTPM

Threat Modelling & Risk Assessment Methodology

This deliverable provides the normative specification of a meta-model which will be used by security analysts in order to capture the cartography of a QR TPM supported environment and the non-normative specification of a multi-step RA methodology that has to be applied prior to the risk quantification. It also provides the approach for integrating multiple levels of risk analysis and dependencies such as safety.

UPCOMING DISSEMINATION ACTIVITIES

Security Research Event (SRE)

05th - 06th December, 2018 | @Brussels, Belgium
Partner RHUL will participate.
www.eu2018.at

PAST DISSEMINATION ACTIVITIES

Security Days for Industry

5th September, 2018 | @ Graz, Austria
Partner IFAT & IFAG participated.
www.securityweek.at

Cyber Security Challenge (CSC)

26th September, 2018 | @ Athens, Greece

The CSC is a series of national competitions, learning programmes, and networking initiatives designed to identify, inspire and enable more people to become cyber security professionals. The University of Piraeus and the UPRC has undertaken the organization and the coordination of the Hellenic participation to CSC.
www.cybersecuritychallenge.org.uk

European Researchers Night

28th September, 2018 | @ Athens, Greece

The Researchers' Night 2018, which was organized in 300 cities around Europe, brought together an unprecedented concentration of technical innovators, media and civil society from all around Europe. The goal was to bring together scientific communities and share state of the art research projects with the rest of the world. Partner UPRC presented the FutureTPM project.
ec.europe.eu

ETSI / IQC Quantum Safe Workshop 2018

7th November, 2018 | @ Beijing, China

Project Partner IFAG has submitted the presenation: "Learning with Errors on RSA Co-Processors" and presented the FuturTPM project at the Workshop.
www.etsi.org

Follow FutureTPM on:

futuretpm.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 779391.