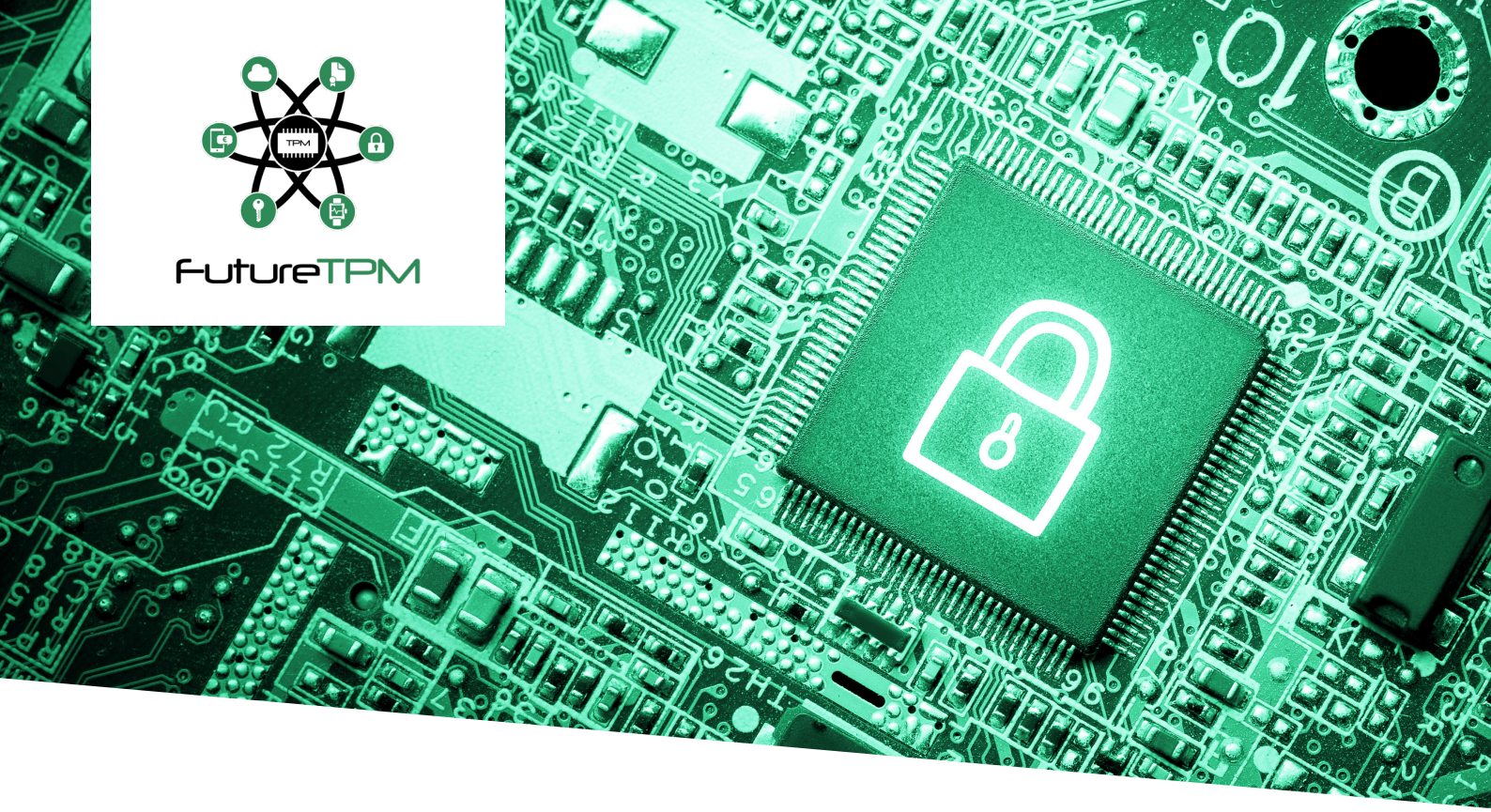


FutureTPM

Newsletter / August 2018 - Issue 2

Future Proofing the Connected World: A Quantum-Resistant Trusted Platform Module

Consortium
14 partners (8 countries)

Project Coordinator
MMAg.[a] Martina TRUSKALLER
coordination@futuretpm.eu

Scientific/Technical Lead
Prof. Liqun CHEN
liqun.chen@surrey.ac.uk

Dr. Thanassis GIANNETSOS
a.giannetsos@surrey.ac.uk

Project number: **779391**
Project website: **futuretpm.eu**
Project start: **1st January, 2018**
Duration: **36 Months**
Total cost: **EUR 4,868,890**
EC contribution: **EUR 4,868,890**

PROJECT STATUS UPDATE

The deliverable **"FutureTPM Use-Cases and System Requirements"** was submitted successfully on July 2nd, 2018. Within this Deliverable the technical requirements, as well as the technical requirements of the whole FutureTPM platform of the envisioned use-cases of Future TPM were defined.

In addition, Milestone MS1 **Availability of the technical and security requirements**, to be met by the FutureTPM framework and the use cases, was achieved successfully.

Milestones MS2 **Availability of the FutureTPM Reference Architecture** and MS3 **Availability of the designed and developed set of QR cryptographic primitives; i.e., symmetric, asymmetric and privacy-preserving - early release** are on track. In addition, preparations for the 1st FutureTPM workshop planned to be on 19th of October started.

Furthermore the FutureTPM consortium is working on the establishment of a cooperation with the Trusted Computing Group ("TCG"), which is a not-for-profit organization, formed to develop, define and promote open, vendor-neutral, global industry standards, supportive of a hardware-based root of trust, for interoperable trusted computing platforms.

FUTURETPM TECHNICAL MEETING IN ATHENS

The first **FutureTPM Technical Meeting** took place in Athens, Greece, from June 13th to 14th, and was hosted by the project partner UBITECH. Initially the meeting was dedicated to a general project status update and an overview of the most important topics, presented by the technical leader.

After this introduction, a workshop on the requirements and characterisation of the FutureTPM started, where the first deliverable (Technical and Security Requirements Analysis) was refined. Additionally, the three use cases online banking, activity tracking and device management were presented, followed by the status report of the deliverable "First Report on New QR Cryptographic Primitives" by IBM.

On the second day, the remaining work packages "QR TPM Integration and Provable Security Modelling and Analysis" and "Run-time Risk Assessment and Vulnerability Analysis" were presented and discussed.

The WP-leaders gave individual project updates and delivered insights into future plans. A final joint session focused on upcoming tasks and the organization of the next technical meeting and workshop took place. Overall, the Technical Meeting was a very successful and engaging event, which provided many useful ideas that will foster further research and developments within the FutureTPM project.

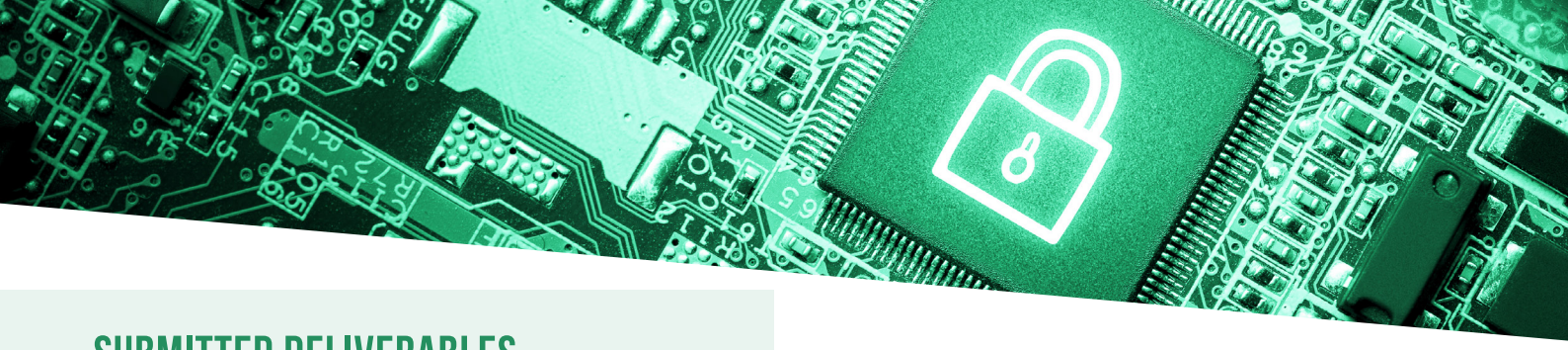
1ST FUTURETPM WORKSHOP

On October 19th, 2018 the 1st FutureTPM Workshop on Quantum-Resistant Crypto Algorithms will take place in Lisbon, Portugal.

Hosted by INESC-ID, it aims at presenting the first set of preliminary results in researching a Quantum-Resistant (QR) Trusted Platform by investigating how existing QR crypto algorithms can be tailored for inclusion in a TPM-type environment; namely hardware-, software- and virtual-TPM. This so-called root-of-trust is commonly used in domains with high security requirements, privacy and trust, such as finance and banking (secure mobile payment), wearables (activity tracking) and device management.

This one-day workshop will bring together diverse players in the quantum-safe cryptography community, with the goal of facilitating knowledge exchange and collaboration to prepare for the advent of the quantum era.

Please Note: There is no registration fee for workshop participants and all necessary material will be provided. As space is limited, please send your confirmation of attendance via email at coordination@futuretpm.eu by August 31st, 2018. For more information please visit the project website!



SUBMITTED DELIVERABLES

Public RTD Deliverables published on FutureTPM

The first deliverable **D1.1** "FutureTPM Use-Cases and System Requirements" was submitted on July 2nd, 2018. Within this Deliverable the technical requirements, as well as the requirements of the use-cases of Future TPM were defined.

UPCOMING PUBLIC DELIVERABLES

Public RTD Deliverables published on FutureTPM

- **D1.2** FutureTPM Reference Architecture
- **D1.3** Security Risks in QR Deployments
- **D2.1** First Report on New QR Cryptographic Primitives
- **D3.1** First Report on Security Models for the TPM

PUBLICATION: LEARNING WITH ERRORS ON RSA CO-PROCESSORS

Martin R. Albrecht, Christian Hanser ,Andrea Hoeller, Thomas Pöppelmann, Fernando Virdia and Andreas Wallner
www.eprint.iacr.org

We repurpose existing RSA/ECC co-processors for (ideal) lattice-based cryptography by exploiting the availability of fast long integer multiplication. Such co-processors are deployed in smart cards in passports and identity cards, secured microcontrollers and hardware security modules (HSM). In particular, we demonstrate an implementation of a variant of the Module-LWE-based Kyber Key Encapsulation Mechanism (KEM) that is tailored for optimal performance on a commercially available smart card chip (SLE 78). To benefit from the RSA/ECC co-processor we use Kronecker substitution in combination with schoolbook and Karatsuba polynomial multiplication. Moreover, we speed-up symmetric operations in our Kyber variant using the AES co-processor to implement a PRNG and a SHA-256 co-processor to realise hash functions. This allows us to execute CCA-secure Kyber768 key generation in 79.6 ms, encapsulation in 102.4 ms and decapsulation in 132.7 ms.

PAST DISSEMINATION ACTIVITIES

ARCH Summit 2018, May 3rd-4th, 2018
@ Luxembourg, Luxembourg
The aim of the event was to bring closer Universities, Start-ups, and investors for future collaborations
www.archsummit.lu

CSIT's 8th World Cyber Security Technology Research Summit, May 9th-10th
@ Belfast, Northern Ireland
www.csit.qub.ac.uk

Partnership Day, June 5th, 2018
@ Luxembourg, Luxembourg
wwwfr.uni.lu

Belfast 2018 Cyber Security Summit, June 9th-10th, 2018
@ Belfast, Northern Ireland
www.csit.qub.ac.uk

TCG f2f meeting, June 20th, 2018
@ San Diego, US
HWDU presented FutureTPM project

ISG Open Day, June 26th, 2018
@ London, UK
www.royalholloway.ac.uk

PLANNED DISSEMINATION ACTIVITIES

1st FutureTPM Workshop, October 19th, 2018
@Lisbon, Portugal
futuretpm.eu

Workshop: Learning with Errors on RSA Co-Processors, November 7th, 2018
@ Beijing, China
www.etsi.org

Workshop: Security Research Event (SRE), December 5th-6th, 2018
@ Brussels, Belgium
www.eu2018.at

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.