FutureTPM

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

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

Daniele Sgandurra (daniele.sgandurra@rhul.ac.uk)

Royal Holloway, University of London, UK

With contributions from Liqun Chen (Univ. of Surrey) and Thanassis Giannetsos (Technical Univ. of Denmark)

International Workshop on CyberSecurity 17th-19th April 2019 – Kyushu University, Kumamoto

FutureTPM general project information

- Project reference: 779391
- Project start: 1st January 2018
- Duration: 3 years
- Total costs/EC contribution:
  EUR € 4,868,890
- 15 partners from 10 different
  European countries
- Website: https://futuretpm.eu/

Consortium

Project Partners:

1 TECHNIKON Forschungs- und Planungsgesellschaft mbH, Austria [Villach]

2 University of Surrey, United Kingdom [Guildford]

3 UBITECH Limited, Cyprus [Limassol]

4 Royal Holloway and Bedford New College, United Kingdom [Egham]

5 IBM Research GmbH, Switzerland [Rüschlikon]

6 The University of Birmingham, United Kingdom [Birmingham]

7 Infineon Technologies AG, Germany [Neubiberg]

8 Infineon Technologies Austria AG, Austria [Graz]

9 Université du Luxembourg, Luxembourg [Luxembourg]

10 Suite5 Data Intelligence Solutions Limited, Cyprus [Nicosia]

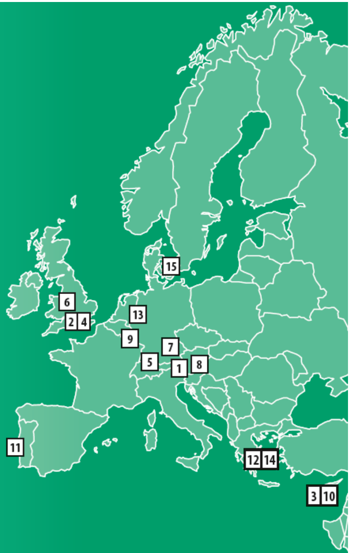
11 INESC-ID – Instituto de Engenhariade Sistemas e Computadores, Investiga-cao e Desenvolvimento em Lisboa, Portugal [Lisboa]

12 University of Piraeus Research Center, Greece [Piraeus]

13 Huawei Technologies Düssel-dorf GmbH, Germany [Düsseldorf]

14 INDEV Software SA, Greece [Athens]

15 Technical University of Denmark, Denmark [Lyngby]



Consortium

The FutureTPM consortium consists of 15 highly qualified industrial and academic partners from a wide variety of back-grounds and from 9 different countries (Austria, Cyprus, Germany, Greece, Lux-embourg, Portugal, Switzerland, United Kingdom and Denmark):

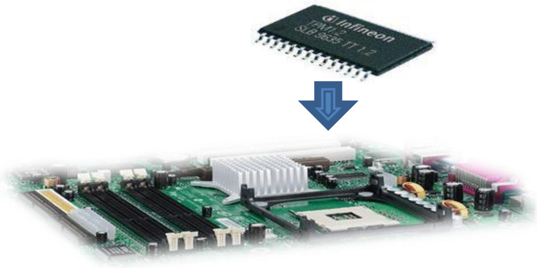
FutureTPM in a nutshell

- Design and develop a **Quantum-Resistant (QR) Trusted Platform Module (TPM)**
- Provide a **new generation of TPM-based solutions,** including hardware, software and virtualization environments
- **Long-term security, privacy** and **operational assurance** for future ICT systems and services
- Improve the security of **Hardware Security Modules**, **Trusted Execution Environments**, **Smart Cards**, and the **Internet of Things**

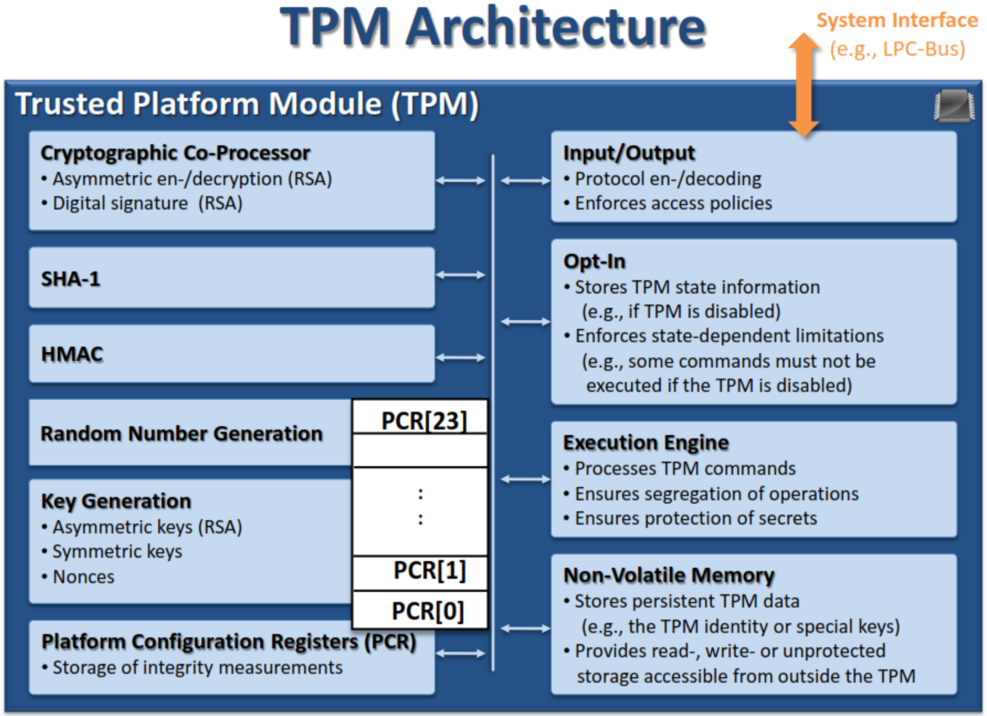
Trusted platform module (TPM)

What is a TPM designed for?

- A **chip** with **low cost**
- **Embedded** in a computing platform
- Serve as a **root-of-trust**
- Make the platform **trustworthy**
- TPM specifications were developed by the **TCG**
- ISO/IEC 11889
- Two versions of TPMs: **1.2** and **2.0**



Simplified architecture of TPM

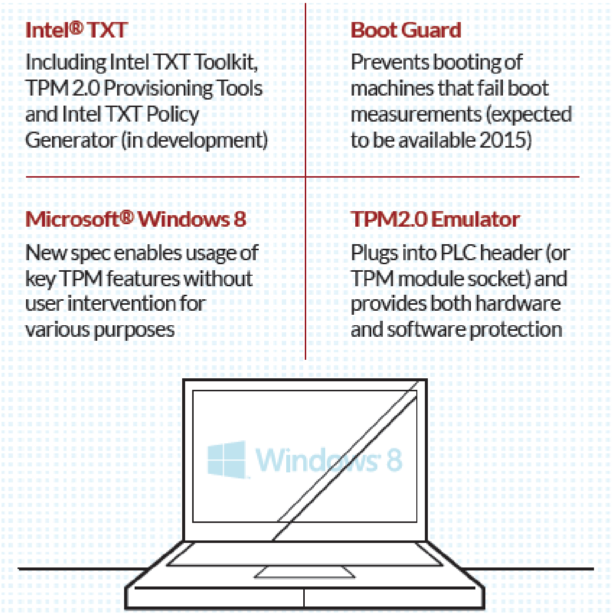


Types of TPMs

TRUST ELEMENT	SECURITY LEVEL	SECURITY FEATURES	RELATIVE COST	TYPICAL APPLICATION
DISCRETE TPM	HIGHEST	TAMPER RESISTANT HARDWARE	$$$	CRITICAL SYSTEMS
INTEGRATED TPM	HIGHER	HARDWARE	$$	GATEWAYS
FIRMWARE TPM	HIGH	TEE	$	ENTERTAINMENT SYSTEMS
SOFTWARE TPM	NA	NA	¢¢	TESTING & PROTOTYPING
VIRTUAL TPM	HIGH	HYPERVISOR	¢	CLOUD ENVIRONMENT

TPM applications

- **Existing applications**:
  - Microsoft **BitLocker, Measured Boot**
  - HP ProtectTools, Embedded Web Server
  - Intel's **Trusted Execution Technology** (**TXT**)
  - Linux Unified Key Setup (**LUKS**)
    - supports storing cryptographic keys in TPMs



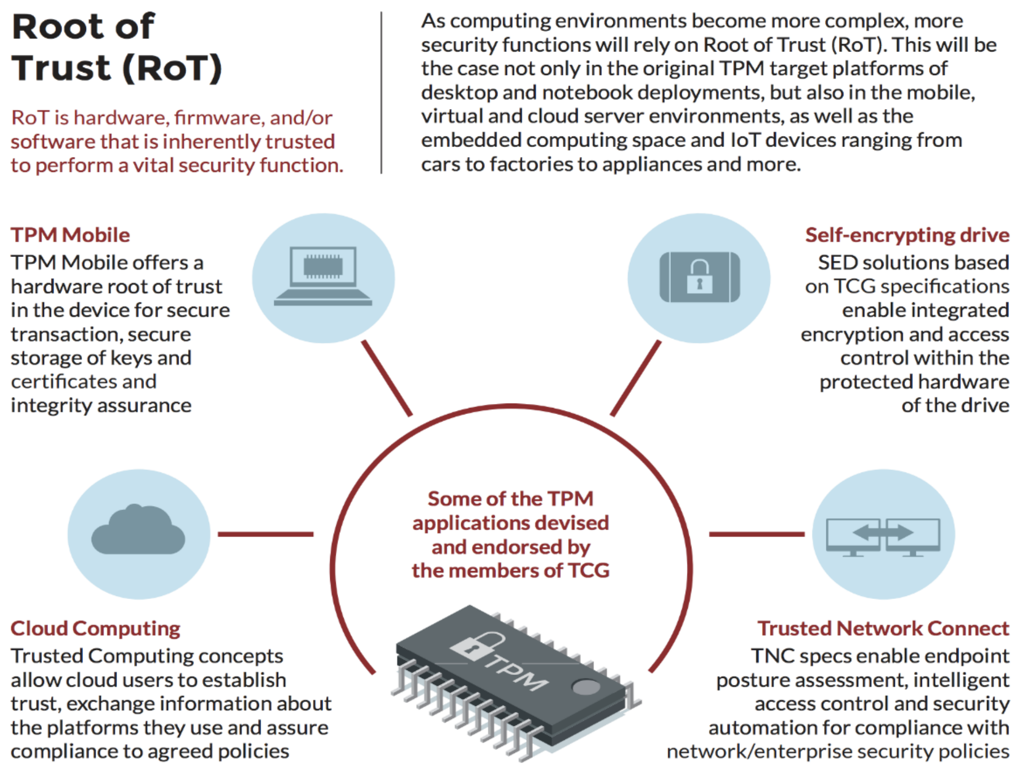
- **Other applications**:
  - TPM in **automotive**
  - TPM in **mobile phones**
  - ……

TPM services

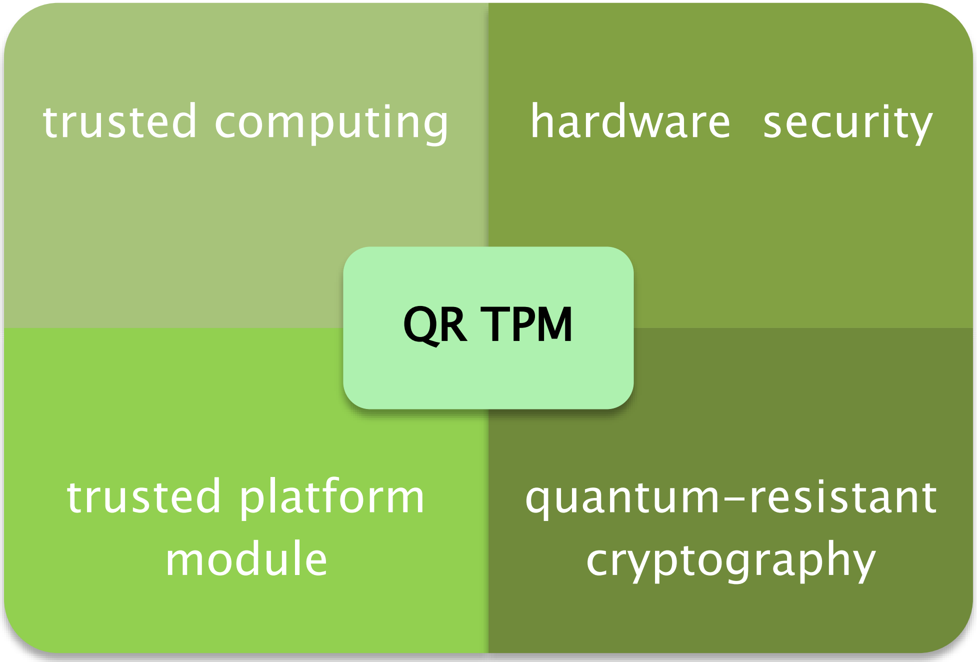
- **Attestation**
- **Protected Storage**
- **Platform Authentication**
- **…**

Cryptographic primitives

- Hash Functions
- Block Ciphers
- Digital Signatures
- Public-key Encryption & Key Exchange
- Direct Anonymous Attestation



Why QR TPM?


trusted computing
hardware security
QR TPM
trusted platform module
quantum-resistant cryptography

Current state: TPM's cryptographic algorithms

Cryptographic Co-processor

- Asymmetric encryption
- Symmetric encryption
- Signatures & DAA
- Message authentication code
- Hash functions
- Key exchange

TPM 1.2 supports

- RSA encryption
- RSA signature
- RSA-DAA
- SHA-1
- HMAC
- AES (optional)

TPM 2.0 supports

- Asymmetric encryption
  - RSA encryption and EC encryption
- Symmetric encryption
  - AES, SM4, Triple DES, …
- Signature
  - RSA signature and EC signature
- DAA
  - EC-DAA
- Message authentication code
  - HMAC
- Hash functions
  - SHA-1, SHA-256, SM3, …
- Key exchange
  - ECDH

When a large-scale quantum computer becomes a reality

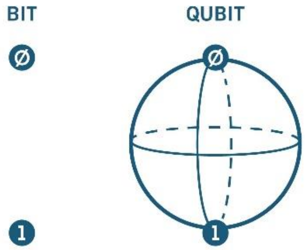
Cryptographic Co-processor
- Asymmetric encryption
- Symmetric encryption
- Signatures & DAA
- Message authentication code
- Hash functions
- Key exchange

TPM 1.2 supports
- RSA encryption BROKEN
- RSA signature BROKEN
- RSA-DAA BROKEN
- SHA-1
- HMAC
- AES (optional)

TPM 2.0 supports
- Asymmetric encryption
  - RSA encryption and EC encryption BROKEN
- Symmetric encryption
  - AES, SM4, Triple DES, …
- Signature
  - RSA signature and EC signature BROKEN
- DAA
  - EC-DAA BROKEN
- Message authentication code
  - HMAC
- Hash functions
  - SHA-1, SHA-256, SM3, …
- Key exchange
  - ECDH BROKEN

Quantum computers

- A classical computer has a memory made up of **bits**
  - each bit is represented by either a 1 or a 0
- A quantum computer, on the other hand, maintains a sequence of quantum bits (**qubits**)
  - can represent a 1, a 0, or any quantum **superposition** of those two qubit states
- A pair of qubits can be in any quantum superposition of 4 states, and three qubits in any superposition of 8 states:
  - in general, a quantum computer with n qubits can be in any superposition of up to 2^n different states
- This compares to a normal computer that can **only** be in one of these 2^n states at any one time.



Quantum computers

Some history:

- 1998 – 2 qubits
- 2000 – 4, 5, and then 7 qubits
- 2006 – 12 qubits
- 2011 – 14 qubits
- 2017 – 17 qubits
- 2018 - Google announces the creation of a 72-qubit quantum chip, called "Bristlecone”

IBM Unveils World's First Integrated Quantum Computing System for Commercial Use

IBM to Open Quantum Computation Center for Commercial Clients in Poughkeepsie, NY

YORKTOWN HEIGHTS, N.Y., Jan. 8, 2019 /PRNewswire/ -- At the 2019 Consumer Electronics Show (CES), IBM (NYSE: IBM) today unveiled IBM Q System One™, the world's first integrated universal approximate quantum computing system designed for scientific and commercial use. IBM also announced plans to open its first IBM Q Quantum Computation Center for commercial clients in Poughkeepsie, New York in 2019.

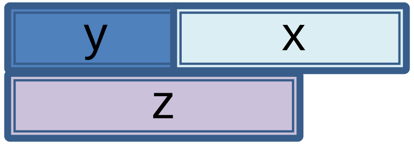
IBM Q systems are designed to one day tackle problems that are currently seen as too complex and exponential in nature for classical systems to handle. Future applications of quantum computing may include finding new ways to model financial data and isolating key global risk factors to make better investments, or finding the optimal path across global systems for ultra-efficient logistics and optimizing fleet operations for deliveries.

Designed by IBM scientists, systems engineers and industrial designers, IBM Q System One has a sophisticated, modular and compact design optimized for stability, reliability and continuous commercial use. For the first time ever, IBM Q System One enables universal approximate superconducting quantum computers to operate beyond the confines of the research lab.

Why now? (1)

Two messages from Dr Michele Mosca, Univ. of Waterloo:

- There is a 1 in 7 chance that **some fundamental public-key crypto will be broken** by quantum by 2026, and a 1 in 2 chance of the same by 2031
- Is this something we need to worry about now? Suppose:
  - we want to keep your information for x years
  - it takes y years to transfer to a QR solution
  - it takes z years to build a large-scale quantum computer



- Theorem: If **x + y > z**, then it is the time to take an action!

Why now? (2)

- It has taken many years to develop the current TPM technology
  - **TCPA** (Trusted Computing Platform Alliance) was formed in 1999, later nearly 200 member companies
  - **TCG** (Trusted Computing Group) was announced in 2003 as the successor to the TCPA
- It will need **many years** to develop
  - The QR cryptographic solutions suitable for inclusion in TPMs
  - The QR TPM specification
  - The QR TPM supporting facilities
- **Now is the time** to begin developing QR technology for TPMs

Three types of TPM QR algorithms

- **Symmetric algorithms**
  - Hash, MAC, symmetric encryption
  - Existing algorithms will not directly be broken, but key/block lengths may need to be increased
- **Conventional asymmetric algorithms**
  - Encryption, signature, key exchange
  - Existing algorithms will be broken
  - Many QR algorithms have been developed (e.g., submissions to NIST PQC)
- **Asymmetric privacy-preserving algorithms**
  - Direct Anonymous Attestation (DAA)
  - Not in the scope of NIST
  - Not much research so far

FutureTPM mission

Mission: *Design a **QR TPM** covering the full range of **implementation environments** coupled with **formal security analysis** and **run-time risk assessment**, and evaluated under assumptions of realistic deployment scenarios*

- Design and development of a holistic TPM-based framework
- Threat security analysis for TPM cryptographic functionality
- Identification and implementation of a reactive, run-time risk assessment model
- Validation of applicability, usability, effectiveness and value of FutureTPM concept

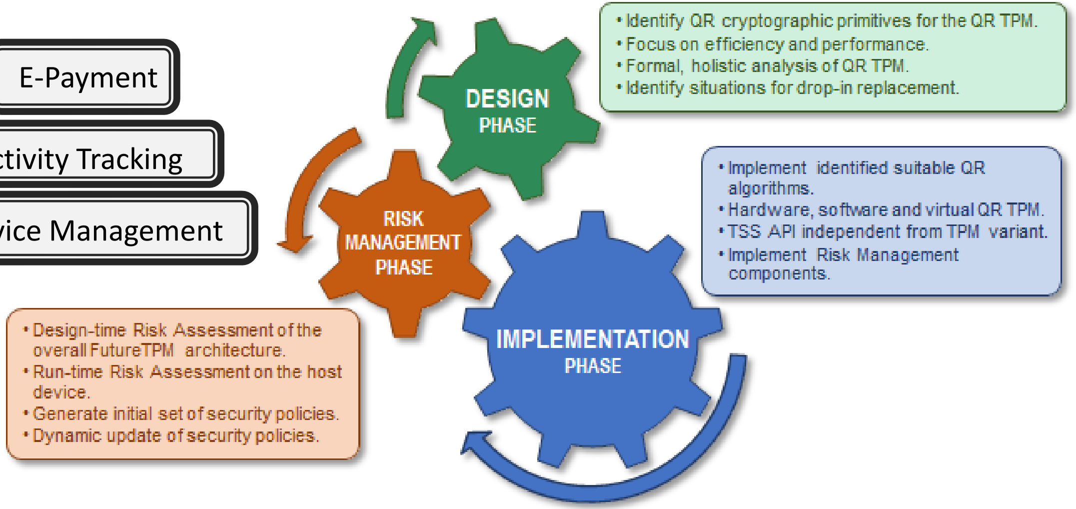
FutureTPM mission (cont)

TPM as a major building block for enhanced security & privacy in various application domains

Secure & Dependable Communication	Authenticity and Integrity	Privacy and Data protection
Security Hardware	Data consistency	Security Architecture

Performance & Efficiency	Cost	Security-Processes/ Management
Security Evolution & Maintenance	Security Metrics	

- E-Payment
- Activity Tracking
- Device Management



Reactive security mechanisms & updates

Project goals

1. Secure Quantum-Resistant Cryptographic Algorithms for the TPM
2. Validation & Verification using Formal Security Analysis
3. Implementation of Hardware, Software, and Virtual TPM
4. Standardization within TCG, ISO/IEC and ETSI
5. Provision of Run-Time Risk Assessment and Vulnerability Analysis Methodologies

Project goal #1

- **Secure Quantum-Resistant Cryptographic Algorithms for the TPM**
  - Identify, design and develop QR algorithms for each cryptographic primitive supported by the current version of TPM
  - Development of bespoke provable-secure quantum-resistant algorithms for
    - Symmetric Cryptography
    - Asymmetric Cryptography
    - Privacy-protecting primitives, such as Direct Anonymous Attestation

Project goal #2

- **Validation & Verification using Formal Security Analysis**
  - Provable security modelling and analysis
  - Define and design appropriate **formal methods**, including computer-aided proof systems and automated proof tools, to support the security analysis model needed to reason about the entire TPM and its functionalities

Project goal #3

- **Implementation of Hardware, Software, and Virtual TPM**
  - Demonstrate the applicability of the identified QR algorithms to the full range of possible TPM environments
  - Implementation and rigorous evaluation of the designed QR algorithms suite in:
    - **hardware TPM (hTPM)**
    - **software TPM (sTPM)**
    - **virtual TPM (vTPM)**

Project goal #4

- **Standardization within TCG, ISO/IEC and ETSI**
  - Development of standardisation proposals that push the state of the art in the areas of cryptography and the TPM itself
  - Involve the technical committees of the relevant standards bodies, notably **ISO, IEC, ETSI** and the **TCG**

NIST PQC standardization process

- NIST received **82 candidate** algorithm submission packages for the NIST PQC Standardization Process
- Of these, NIST accepted **69 first-round candidates**
- NIST selected **26 second-round candidates** from the 69 first-round candidates

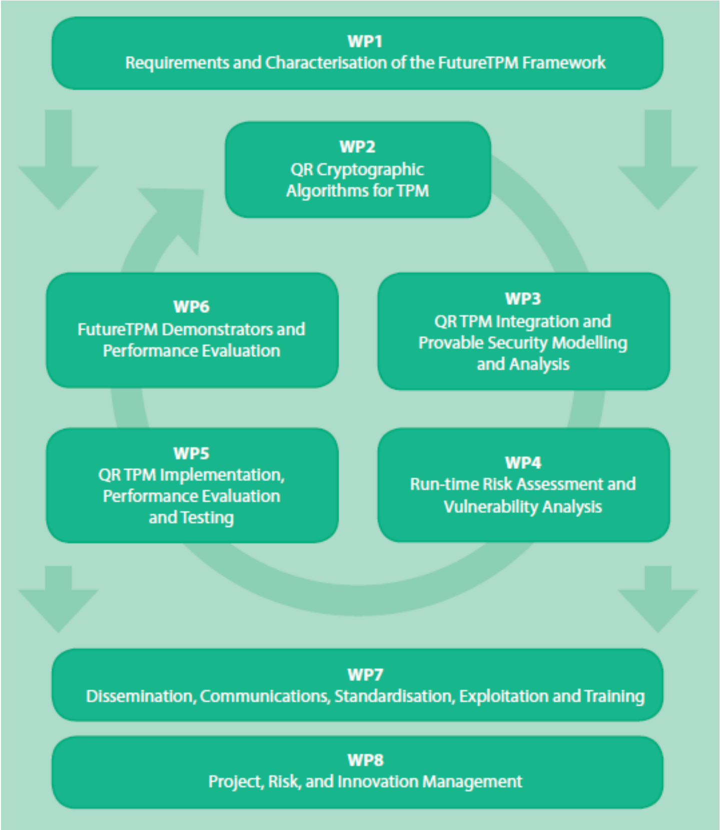
Second Round Candidates

BIKE	LEDAcrypt	Rainbow
Classic McEliece	LUOV	ROLLO
CRYSTALS-DILITHIUM	MQDSS	Round5
CRYSTALS-KYBER	NewHope	RQC
FALCON	NTRU	SABER
FrodoKEM	NTRU Prime	SIKE
GeMSS	NTS-KEM	SPHINCS+
HQC	Picnic	Three Bears
LAC	qTESLA	

Project goal #5

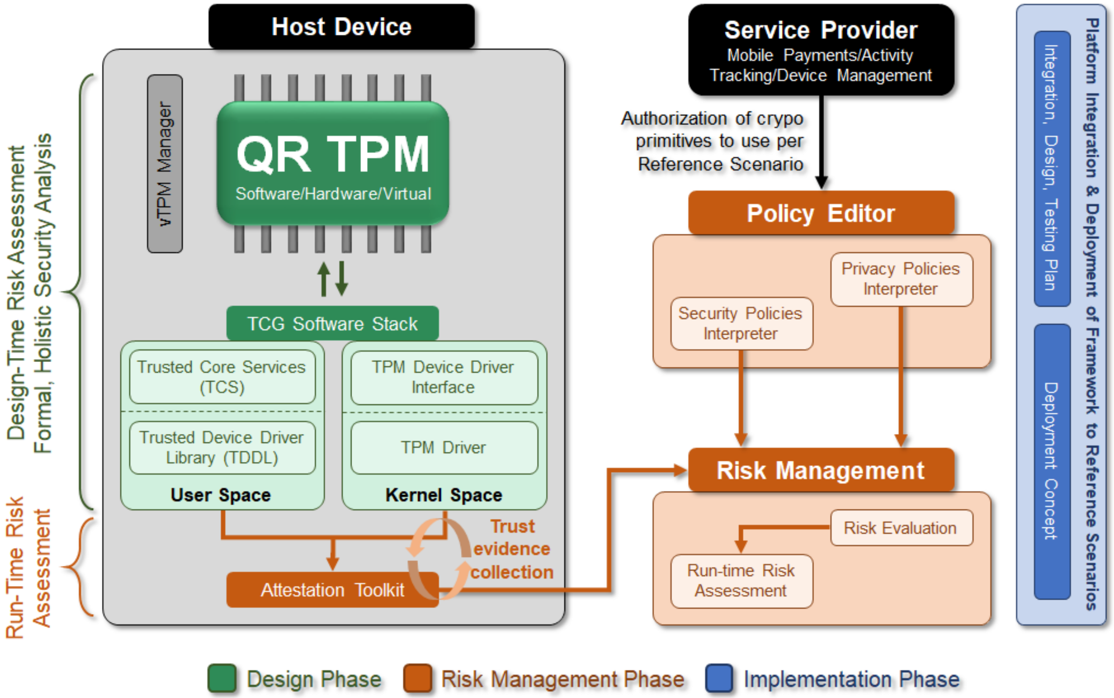
- **Provision of Run-Time Risk Assessment and Vulnerability Analysis Methodologies**
  - FutureTPM will design **risk analysis methods** that target all the phases of a system's development lifecycle, from design time to near real-time risk quantification of newly identified attacks

WPs interaction



FutureTPM conceptual architecture

- **FutureTPM QR Design:**
  - QR Crypto Primitives
- **FutureTPM Implementation:**
  - HW, SW, VM-based
  - Secure Storage, Attestation
- **Risk Management:**
  - Risks, threats, assets, attack types, vulnerabilities, control elements
  - Fine-grains security policies
- **Security Modelling:**
  - Threats (physical/software/remote) to be considered



FutureTPM use cases

Online Banking

- To isolate the e-payment process in a more protected context so as to provide enhanced security levels against unintentional data leakage and malicious apps

Activity Tracking

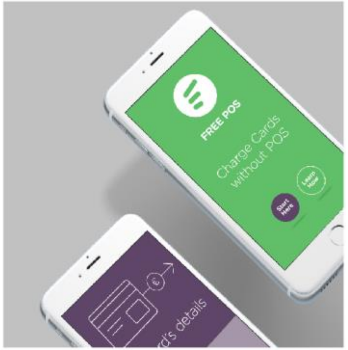
- To increase the trust of users of cloud-based activity tracking services in the security and privacy properties of their stored and leveraged data

Device Management

- To help protect private keys stored on routers, mobile devices, and IoT devices against compromise or misuse by malicious applications

Secure mobile wallet and payments

- Use of **FreePOS** application as a testbed developed by **INDEV, GR**
  - One of the top finance apps in Greece – tens of thousands active users
  - **Hardware-based TPM**
- **Token-based** authentication
  - *Depends on OS level security*
- OAuth 2.0 with PCI compliant services



- **Confidentiality**
  - TPC key storage persistency -> token storage
- **Integrity**
  - HMAC digital signatures for financial data integrity
- **Authentication**
- **Key Exchange**

Personal activity and health kit data tracking

- Use of **S5 Tracker** application as a testbed developed by **SUITE5 Data Intelligence Solutions, UK**
- **Data Anonymization** and **Privacy Preservation**
  - *Generation of "User Personas"*
  - **Software-based TPM**
- **Privacy**, confidentiality and security at the edge
  - Direct Anonymous Attestation
- **Data Integrity**
  - HMAC digital signatures for financial data integrity
- **Secure Data Sharing**
  - No data leakage

Device management

- **Secure management** of network infrastructures by HWDU
  - Integrity of identified devices
  - **Virtual-based TPM**
- **Device Identification:**
  - *TPM key generation and persistent storage*
- **Software Integrity**
  - TPM Platform Configuration Registers (PCRs)
- **Data Integrity and Confidentiality**
  - Key usage TPM policies

2-phase testing

- **1st Phase Testing:**
  - Internal, small-scale, lab-test
  - **M18** (MS4) - first release of SW-based TSS + QR TPM + RA framework
  - **M21** (MS5) - first release of FutureTPM framework
  - **M24** – 1st Demonstration Phase + 2nd FutureTPM Workshop
- **2nd Phase Testing:**
  - Internal, large-scale, hybrid test
  - **M27** (MS7) – Final release of FutureTPM framework (including all TPM implementations)
  - **M33** (MS8) – 2nd Demonstration Phase + 3rd FutureTPM Workshop

QR-TPM implementations

- Evaluate different PQC algorithms in 3 demonstrators:
  - SW-based
    - Kyber, Dilithium, DAA
  - Virtual
    - Kyber, Dilithium, DAA *(inherited from SW-TPM)*
    - + BIKE, SPHINCS+
  - HW-based
    - NewHope, qTesla

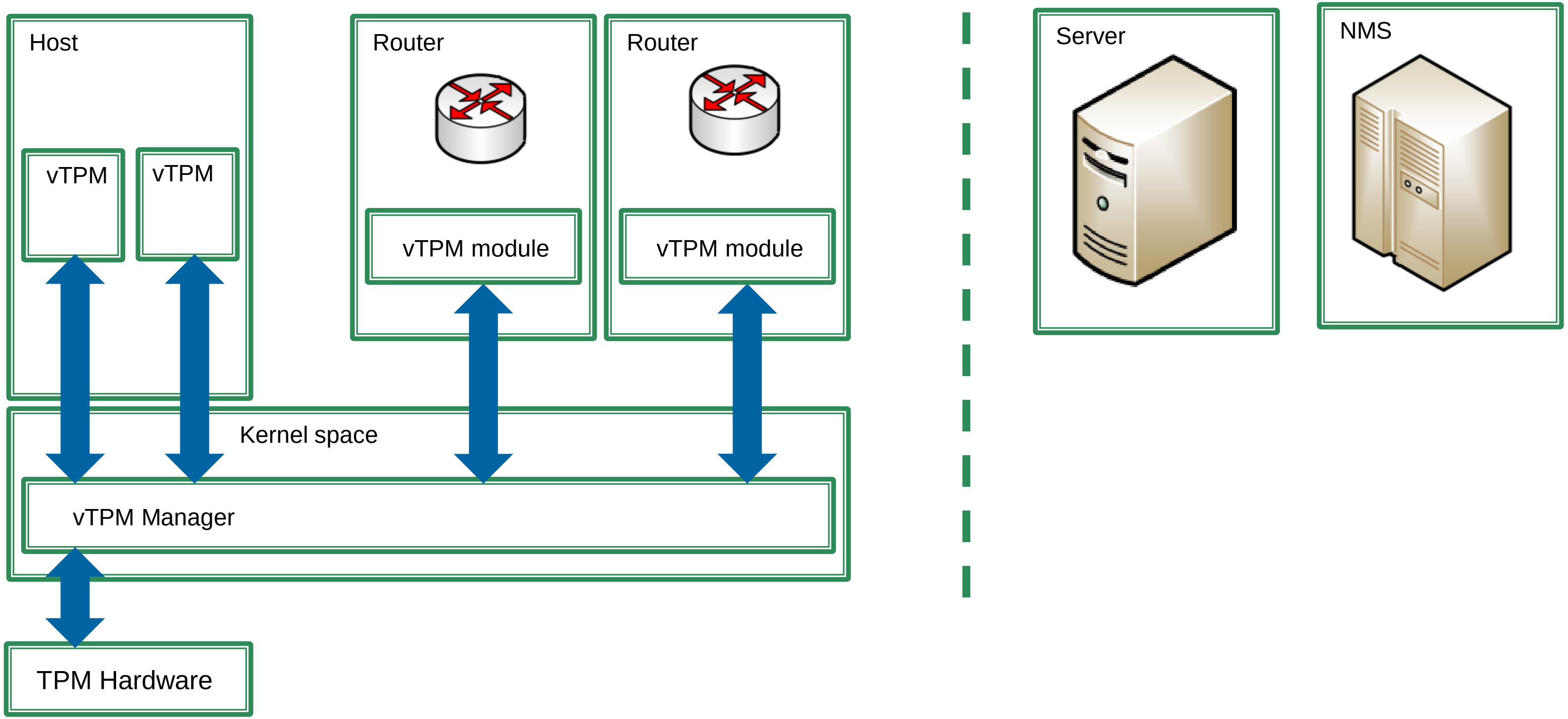
Royal Holloway Main Activities in FutureTPM

- **Research activities**:
  - functional and security requirements of qTPM
  - virtual qTPM (**vTPM**)
- **Dissemination activities**:
  - WP7 leader
    - meetings
    - workshops
    - material
      - leaflets
      - logos
      - poster

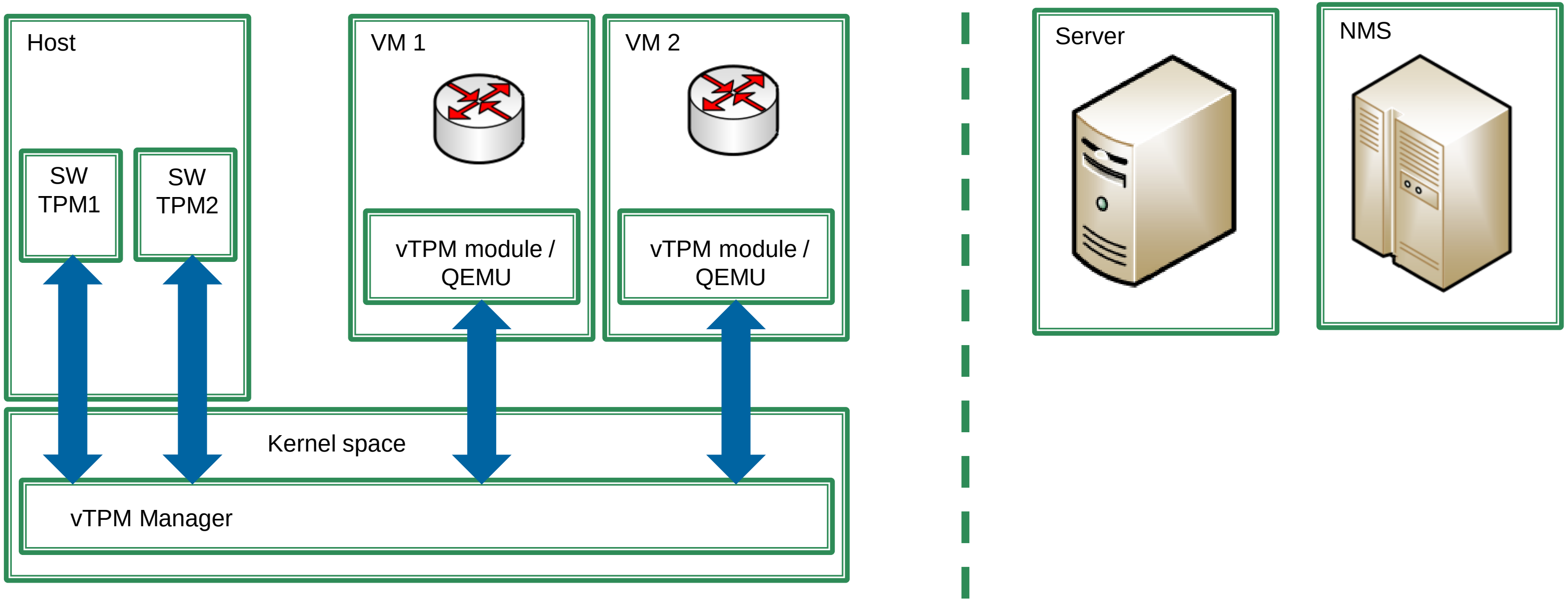
vTPM approach & security features

- **Develop vTPM on KVM:**
  - Proof-of-concept targeted at use-case specific functionalities
  - But generic enough to be used for other scenarios
- **Intended security features:**
  - vTPM isolation
  - Key secure storage (outside the TPM)
- **Additional security features**:
  - Secure migration

vTPM (on KVM) mapped to use case



vTPM (on KVM) architecture with SW-TPM



Dissemination activities so far

- Three **newsletters** + 1 ongoing
- Five **project meetings** + 1 next
- 1 **workshop** + 1 planned research workshops
- 6 public **deliverables** + 3 ongoing
- Etc.

- Everything is **available on the website** (https://futuretpm.eu) together with leaflets (long and short) and various information (e.g., events)

Dissemination activities so far

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

FutureTPM

HOME PRESS & NEWS EVENTS RESULTS BLOG PARTNERS RELATED PROJECTS

PUBLIC RTD DELIVERABLES

D1.1 FutureTPM Use Case and System Requirements || M06

This deliverable defines the technical requirements of FutureTPM, alongside with the requirements of the use cases. Its purpose to define the parameters for the rest of the FutureTPM project and provide the necessary input to the architecture.

Download D1.1 FutureTPM Use Case and System Requirements [PDF, 1.15 MB]

D1.2 FutureTPM Reference Architecture || M09

This deliverable will provide the specification of the FutureTPM reference architecture, the functional components and interfaces between them. It will provide an analysis and point of reference for the FutureTPM in relation to the three specific use cases, including an analysis of relevant classical protocols and the use cases themselves in terms of FutureTPM functionality.

D1.3 Security Risks in QR Deployments || M09

This deliverable will include a documentation of the security problems and risks that classical protocols, to be employed in the three envisioned use cases, might face in the presence of quantum adversaries.

D2.1 First Report on New QR Cryptographic Primitives || M09

This deliverable reports on the work done by all tasks, including the surveys, the newly developed algorithms, and the full specification of the candidate algorithms (TPM and TSS) that are to be implemented and evaluated by WP5.

D3.1 First Report on Security Models for the TPM || M09

Initial report describing and outlining security models for various implementations of TPM.

D1.1: FutureTPM use case and system requirements

FutureTPM

D1.1

FutureTPM Use Cases and System Requirements

Project number:	779391
Project acronym:	FutureTPM
Project title:	Future Proofing the Connected World: A Quantum-Resistant Trusted Platform Module
Start date of the project:	1st January, 2018
Duration:	36 months
Programme:	H2020-DS-LEIT-2017

Deliverable type:	Report
Deliverable reference number:	DS-06-779391 / D1.1/ 1.0
Work package contributing to the deliverable:	WP 1
Due date:	Jun 2018– M06
Actual submission date:	2nd July, 2018

Responsible organisation:	S5
Editor:	Minas Pertselakis, Ioanna Michael, Dimitris Panopoulos
Dissemination level:	PU
Revision:	1.0

Abstract:	D1.1 defines the technical requirements of FutureTPM, alongside with the requirements of the use cases. Its purpose to define the parameters for the rest of the FutureTPM project and provide the necessary input to the architecture.
Keywords:	Requirements, Technical Requirements, Use Cases, user Stories, MVP, Vision

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

Digital Signature Schemes

All the proposed schemes have been submitted to the NIST Post-Quantum Standardization process.

Proposed Candidates

- **Dilithium** is a lattice-based signature from NTRU assumption. It is based on the Fiat-Shamir with Aborts approach which uses rejection sampling to make Fiat-Shamir schemes compact and secure. It can achieve 1,2 and 3 of NIST security categories.
- **Tesla** is based on the hardness of the decisional RLWE problem. It can achieve 1,3, and 5 level of NIST security categories.
- **pqNTRUSign** is a lattice-based signature scheme based on NTRU assumptions. It is based on hash-and-sign construction and it can achieve all 5 NIST security categories.
- **FALCON** is a lattice-based signature scheme from NTRU assumptions. It is based on the theoretical framework of Gentry, Peikert and Vaikuntanathan and it is underlying hard problem is the short integer solution problem (SIS) over NTRU lattices. It can achieve all 5 NIST security categories.
- **SPHINCS** is a hash-based algorithm that relies solely on the security of the underlying cryptographic hash function. It is a stateless protocol and can be a drop-in replacement for RSA and ECDSA.

Remarks: it is difficult to understand if the schemes are efficient enough to be included in FutureTPM. In addition, finding the right balance between quantum-resistant levels (QS1 or QS2) and performance is not trivial.

D1.2: FutureTPM reference architecture

FutureTPM

D1.2

FutureTPM Reference Architecture

Project number:	779391
Project acronym:	FutureTPM
Project title:	Future Proofing the Connected World: A Quantum-Resistant Trusted Platform Module
Start date of the project:	1st January, 2018
Duration:	36 months
Programme:	H2020-DS-LEIT-2017

Deliverable type:	Report
Deliverable reference number:	DS-06-779391 / D1.2 / 1.0
Work package contributing to the deliverable:	WP 1
Due date:	Sept. 2018 – M09
Actual submission date:	3rd October, 2018

Responsible organisation:	UB
Editor:	Jose Moreira (UB) Thanassis Giannetsos, Liqun Chen (SURREY)
Dissemination level:	PU
Revision:	1.0

Abstract:	Deliverable D1.2 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.
Keywords:	Architecture Specification, Functional Components, Interfaces & APIs, Requirements Analysis, TPM Specification.

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

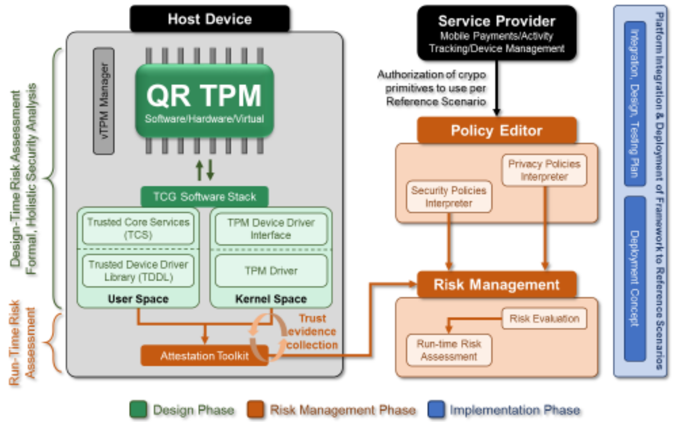


Figure 7: FutureTPM conceptual architecture.

Recall that the specific details of the implementation of the inputs and outputs for each component, and how they are going to be expressed will be made precise in the contexts of WP6. More specifically, in Deliverable D6.1 - Technical Integration Points and Testing Plan, where a detailed guideline will be provided, relating of how the different implementation components are going to be integrated and communicate with each other.

Table 17 summarizes the communication flow, the types of inputs and outputs expected, and where the concrete instantiations of the messages will be defined.

D1.3: Security risks in QR deployments

FutureTPM

D1.3
Security Risks in QR Deployments

Project number:	779391
Project acronym:	**FutureTPM**
Project title:	Future Proofing the Connected World: A Quantum-Resistant Trusted Platform Module
Project Start Date:	1st January, 2018
Duration:	36 months
Programme:	H2020-DS-LEIT-2017
Deliverable Type:	Report
Reference Number:	DS-LEIT-779391 / D1.3 / v1.0
Workpackage:	WP 1
Due Date:	30th September, 2018
Actual Submission Date:	28th September, 2018
Responsible Organisation:	UL
Editor:	Alfredo Rial
Dissemination Level:	PU
Revision:	v1.0
Abstract:	We analyze how the security of current TPM deployments would be affected if sufficiently large quantum computers were available. First, we recall the quantum algorithms that are relevant to cryptography. Then we analyze how the security of many currently deployed cryptographic schemes would be affected if we had sufficiently large quantum computers. Finally, we describe in more detail the security risks that would arise in the event of quantum adversaries in the three-use cases of the FutureTPM project: e-payment, activity tracking and device management.
Keywords:	quantum computing, quantum algorithms, security analysis

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

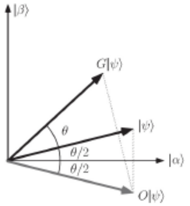


Figure 3.10: The action of a Grover iteration. First, the oracle O reflects the state vector $|\psi\rangle$ about the state $|\alpha\rangle$. Second, the operation $2|\psi\rangle\langle\psi| - I$ reflects the result about $|\psi\rangle$.

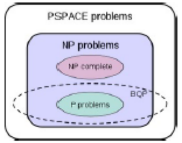


Figure 3.11: Relation between BQP and classical complexity classes.

$|\alpha\rangle$ and $|\beta\rangle$ about the vector $|\psi\rangle$. The product of this two reflections is a rotation. Both reflections are depicted in Figure 3.10. Let $\cos\theta/2 = \sqrt{(N-M)/N}$, so that $\psi = \cos(\theta/2)|\alpha\rangle + \sin(\theta/2)|\beta\rangle$. The rotation angle is θ. After k applications of the Grover iteration, the state is

$$G^k|\psi\rangle = \cos\left(\frac{2k+1}{k}\theta\right)|\alpha\rangle + \sin\left(\frac{2k+1}{2}\theta\right)|\beta\rangle$$

Therefore, repeated applications of G gets the state closer to $|\beta\rangle$. When G is repeated sufficient times, a measurement outputs with high probability one of the solutions to the search problem superposed in $|\beta\rangle$. A performance analysis indicates that $O(\sqrt{N/M})$ Grover iterations are sufficient, in contrast to $O(N/M)$ oracle calls required in a classical computer. It is proven that Grover's algorithm is asymptotically optimal [2].

D2.1: First report on new QR cryptographic primitives

FutureTPM

D2.1

First Report on New QR Cryptographic Primitives

Project number:	779391
Project acronym:	**FutureTPM**
Project title:	Future Proofing the Connected World: A Quantum-Resistant Trusted Platform Module
Project Start Date:	1st January, 2018
Duration:	36 months
Programme:	H2020-DS-LEIT-2017
Deliverable Type:	Report
Reference Number:	DS-LEIT-779391 / D2.1 / v00.01
Workpackage:	WP 2
Due Date:	September 30, 2018
Actual Submission Date:	August 30, 2018
Responsible Organisation:	IBM
Editor:	Tommaso Gagliardoni
Dissemination Level:	PU
Revision:	v00.01
Abstract:	In this document we begin the analysis of quantum-resistant cryptographic primitives in respect to their use in FutureTPM. The final goal is to identify suitable algorithms for adoption in the FutureTPM specification.
Keywords:	quantum security, quantum resistant, post-quantum, cryptography, primitives, QR

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

5.2.1.2 PQ security

The support for QR primitives is one the main cornerstones of FutureTPM. To future-proof the TPM in the context of quantum computers which will break many aspects of conventional cryptography, the primitives listed above must be resistant to attack by quantum computers.

- *[SR.1.2.1]* Support for possible QR-crypto candidates for each category (symmetric, asymmetric and DAA);
- *[SR.1.2.2]* QR Support for signing, key exchange, attestation;
- *[SR.1.2.3]* Reach QS-Level 1 (post-quantum crypto);
- *[SR.1.2.4]* Provide a crypto library with TPM backed keys implementing TLS with QR algorithms.

5.2.1.3 Integrity requirements

One of the main functionalities of TPMs is related to software integrity. This includes verifying that the software running on a device is trustworthy and has not been tampered with by intruders or malware. Therefore, FutureTPM must offer the same functionality of TPM 2.0:

- *[SR.1.3.1]* Support software measurement (PCR extend) and measurement reporting (Quote), using QR algorithms;
- *[SR.1.3.2]* Support remote attestation functionalities;
- *[SR.1.3.3]* Support sealing and binding operations.

5.2.1.4 Data privacy

One key aspect of future TPM is the privacy guarantees of the data stored. At base, this is the goal of any cyber security system, ensuring your data is protected from intruders, which the TPM seeks to enable even if the device as a whole may be compromised.

- *[SR.1.4.1]* Allow the protection of sensitive information;
- *[SR.1.4.2]* It should be hard for an adversary to learn the secret information required for any action (e.g., authentication, encryption, etc.);
- *[SR.1.4.3]* Credentials should be stored on user device and must be protected from eavesdropping/leakage.

5.2.2 Desirable Security Requirements

D3.1: First report on security models for the TPM

FutureTPM

D3.1

First Report on Security Models for the TPM

Project number:	779391
Project acronym:	**FutureTPM**
Project title:	Future Proofing the Connected World: A Quantum-Resistant Trusted Platform Module
Project Start Date:	1st January, 2018
Duration:	36 months
Programme:	H2020-DS-LEIT-2017
Deliverable Type:	Report
Reference Number:	DS-LEIT-779391 / D3.1 / v1.0
Workpackage:	WP 3
Due Date:	Sept. 2018 - M09
Actual Submission Date:	1st October, 2018
Responsible Organisation:	SURREY
Editor:	François Dupressoir
Dissemination Level:	PU
Revision:	v1.0
Abstract:	In this report, we review the FutureTPM requirements and identify effects on design and modelling targets and challenges. We then review the state of the art in threat and security modelling, in general and as applied to the TPM and other similar TEEs. We end the report by summarizing our findings, as well as planning and delimiting the research to be performed.
Keywords:	requirements, threat modelling, security modelling

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

Functionalities	Dependencies: Internal	Dependencies: External
Cryptography	• **Random Number Generation** for strong and secure key generation. • **Message Authentication Codes** for key generation and key derivation. • **Asymmetric Cryptography** for digital signatures. • **Hash Functions** for the functionality of Message Authentication Codes.	• **Entropy Collection** from a reliable and high entropy source, in order for random number generation to be secure.
Storage	• **Symmetric Cryptography** for secure storage to encrypt sensitive data. • **TPM protections** that will enforce proper access control on non-volatile memory. • **Hash Functions** which are used for the calculation of the values in platform configuration registers.	
Authorization	• **Message Authentication Codes** that are used for the authentication of each command. • **PCR Storage** that is used to prove the state of the machine while issuing commands. • **External Authentication Devices** which will prove the identity of the user.	
Attestation	• **Asymmetric Cryptography and Signing Schemes** are needed to sign the values of PCRs in order to prove the valid state of the device. • **PCR Storage** that hold hash values calculated on the state of the device.	
Privacy	• **Asymmetric Cryptography** that is used to sign messages to prove the authenticity of the TPM. • **Key Derivation** which will be used to generate Attestation Identity Keys in order to ensure the privacy of the device. • **Direct Anonymous Attestation** that replaces Attestation Identity Keys and also ensures the privacy of the device.	

Table 2.1: Summary of TPM Functionality Dependencies

D4.1: Threat modelling & risk assessment methodology

FutureTPM

D4.1

Threat Modelling & Risk Assessment Methodology

Project number:	779391
Project acronym:	FutureTPM
Project title:	Future Proofing the Connected World: A Quantum-Resistant Trusted Platform Module
Start date of the project:	1st January, 2018
Duration:	36 months
Programme:	H2020-DS-LEIT-2017

Deliverable type:	Report
Deliverable reference number:	DS-06-779391 / D4.1 / 1.0
Work package contributing to the deliverable:	WP 4
Due date:	Dec 2018 – M12
Actual submission date:	6th February, 2019

Responsible organisation:	UBITECH
Editor:	Sofianna Menesidou (UBITECH)
Dissemination level:	PU
Revision:	1.0

Abstract:	Deliverable D4.1 provides the details of the Risk Assessment (RA) methodology that will be followed in FutureTPM towards the design and implementation of a holistic RA framework capable of providing *vulnerability analysis* and *policy enforcement* during both **design-** and **run-time**. It also provides the analysis of the TPM commands that will be used as the baseline for our investigation (per reference scenario). Each reference scenario will focus on one main TPM functionality including *Sealing*, *Direct Anonymous Attestation* (DAA) and *Key Creation and Storage*.
Keywords:	Risk Assessment, Threat modelling, Vulnerability Analysis, Mitigation Enforcement, Control Flow Integrity, extended Berkeley Filters, Policy Enforcement

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

D4.1 – Threat Modelling & Risk Assessment Methodology FutureTPM

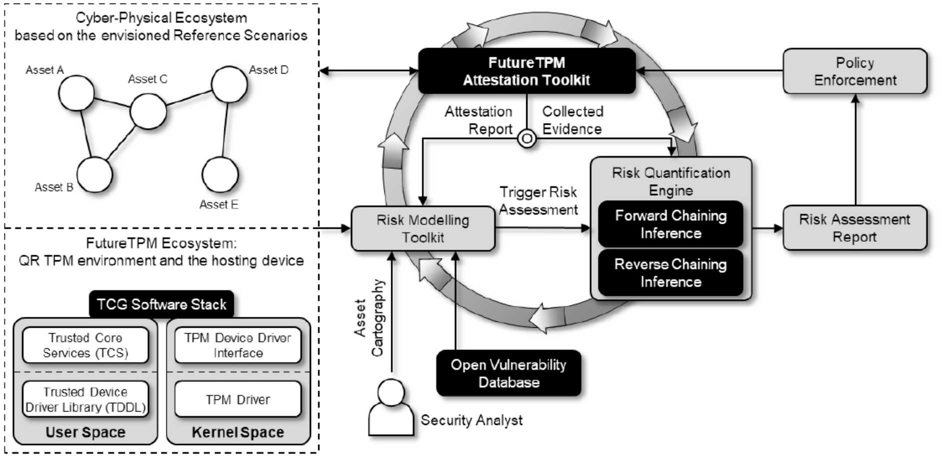


Figure 5: Risk Assessment Framework.

Workshop #1

- The **1st FutureTPM Workshop on Quantum-Resistant Crypto Algorithms** was held in Lisbon on the 19th of October 2018. 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 participants** 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

Workshop #2 (Tentative)

- Workshop on **Cyber-Security Arms Race (CYSARM)**
  - **General Chair:** Chris Mitchell and Liqun Chen
  - **Program Chairs:** Thanassis Giannetsos and Daniele Sgandurra
- **Co-located to a cyber-security conference (to be confirmed)**
- **Topics** of interest include but are not limited to:
  - Advanced cryptographic techniques (e.g., homomorphic encryption, secure multi-party computation and differential privacy)
  - Arms races and trade-offs in cyber-security (e.g., attackers vs defenders, security vs privacy, security vs trust, security vs usability, etc.)
  - Double-edged sword techniques in cyber-security (e.g., artificial intelligence)
  - Impact of quantum computing on cyber-security (not limited to cryptography)
  - Next-generation trustworthy computing security solutions and attacks (e.g., TPMs, TEEs, SGX, SE), and their impact
  - Novel attacks and protection solutions in mobile, IoT and Cloud
  - Post-quantum cryptography
  - Security analysis of protocols, including use of formal techniques
  - Standardization of cyber security and trust techniques
  - Validation of cyber-security technologies

Other post-quantum crypto projects

- **PQCRYPTO**
  - Design of high-security post-quantum PK systems
- **SAFECrypto**
  - Practical, robust and physically secure post-quantum crypto solutions
- **PROMETHEUS**
  - Quantum-resistant privacy-preserving cryptographic mechanisms

Logo

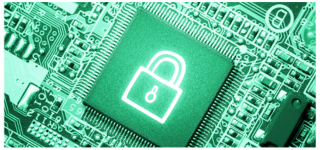
FutureTPM

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

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

Mission

The **FutureTPM** project is aimed at designing and developing a Quantum-Resistant (QR) Trusted Platform Module (TPM).



This will allow long-term **security, privacy** and **operational assurance** for future ICT systems and services.

Approach

FutureTPM will design an innovative portfolio of **high security QR algorithms** for security primitives, such as:

- Key Agreement
- Encryption
- Signature
- Cryptographic Hashing
- Message Authentication Code
- Direct Anonymous Attestation

This will enable FutureTPM systems to generate a **secure root of trust** for a wide range of ICT services.

Use Cases

Online Banking: to isolate the e-payment process in a more protected context to provide enhanced security

Activity Tracking: to increase the trust of users of cloud-based activity tracking services

Device Management: to protect keys on routers, mobile devices, and IoT

Standardisation

Planned outcomes include the development of **standardisation** proposals to push the state of the art in cryptography and the TPM.

They will involve the technical committees of relevant standards bodies: **ISO, IEC, ETSI** and the **TCG**.

Main Goals

- Secure QR Cryptographic Algorithms for the TPM
- Implementation of Hardware, Software, and Virtual TPM
- Design Validation using Formal Security Analysis
- Run-Time Risk Assessment and Vulnerability Analysis

Contact Information

Web: https://futuretpm.eu/
Email: coordination@futuretpm.eu
Project Coordinator: Technikon
Scientific Lead: University of Surrey

Hiring ☺

- **Post-Doctoral Research Associate**
  - Fixed Term Contract for 20 Months
  - Research on vTPM-based security (e.g., secure migration), and on dissemination and standardization activities of the project
- **Research Assistant for Virtual TPM Development**
  - Fixed Term Part-Time (20 hours a week, 4 month period – 8 months)
  - Development of a virtual quantum-resistant TPM for KVM

Conclusion

- FutureTPM will provide a **new generation of TPM-based solutions**
- FutureTPM will fill the gaps that currently threaten the long-term security properties of trusted computing
- Will enable FutureTPM systems to **generate a secure root of trust** that can be used
  - for interacting with Cloud services
  - accessing corporate services
  - performing banking and eCommerce transactions
  - along with a wide range of other services

FutureTPM Project Contacts

Project Coordinator

MMag. Martina Truskaller
TECHNIKON Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a
9500 Villach, Austria
Tel.: +43 4242 233 55
Email: cooridnation@futuretpm.com

Website: https://futuretpm.eu/

- FutureTPM_H2020 — FOLLOW US ON twitter
- FutureTPM-Project — LinkedIn

Technical Leader

Prof. Liqun CHEN
University of Surrey
388 Stag Hill
Guildford GU2 7XH
United Kingdom
Email: liqun.chen@surrey.ac.uk

and Dr. Thanassis GIANNETSOS
Technical University of Denmark
Anker Engelunds Vej 1 Bygning 101A,
2800 Kgs. Lyngby, Denmark
Email: atgi@dtu.dk

FutureTPM Grant Agreement No. 779391

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

If you need further information, please contact the coordinator:

TECHNIKON Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a, 9500 Villach, AUSTRIA
Tel: +43 4242 233 55 Fax: +43 4242 233 55 77
E-Mail: coordination@futuretpm.eu