


# The Impacts of Post Quantum Cryptography

Creating Trust in  
the Digital Society

The logo for utimaco, featuring the word "utimaco" in a bold, black, sans-serif font. A small blue diamond is positioned above the letter 'i'. A registered trademark symbol (®) is located at the top right of the word.

A man with dark hair and glasses, wearing a grey suit jacket over a light blue and white checkered shirt, is speaking. He is positioned on the left side of the frame. A large blue diamond graphic is overlaid on the right side, containing white text. The background is a blurred outdoor setting with stone walls and arches.

“ Quantum  
Computing will  
decimate the security  
infrastructure of the  
digital economy ”

**Dr. Michele Mosca**

Founder of the Institute for Quantum Computing,  
University of Waterloo

## The Impacts of Quantum Computing on Applications and Use Cases

### Impersonation

- ◆ Attacker “calculates” secret credentials of your PIV or EMV card from publicly available information and authenticates as you
- ◆ Attacker approves requests and/or signs documents in your name



### Fake identities

- ◆ Issuance of fake certificates (i.e. identities) in the name of your organization's PKI



### Document / data manipulation

- ◆ Attacker manipulates documents w/o invalidating their signature
- ◆ Attacker manipulates blockchains, e.g. Bitcoin to steal your money



### Eavesdropping

- ◆ Record key agreement (e.g. TLS) today, break it in 15 years to decrypt confidential information



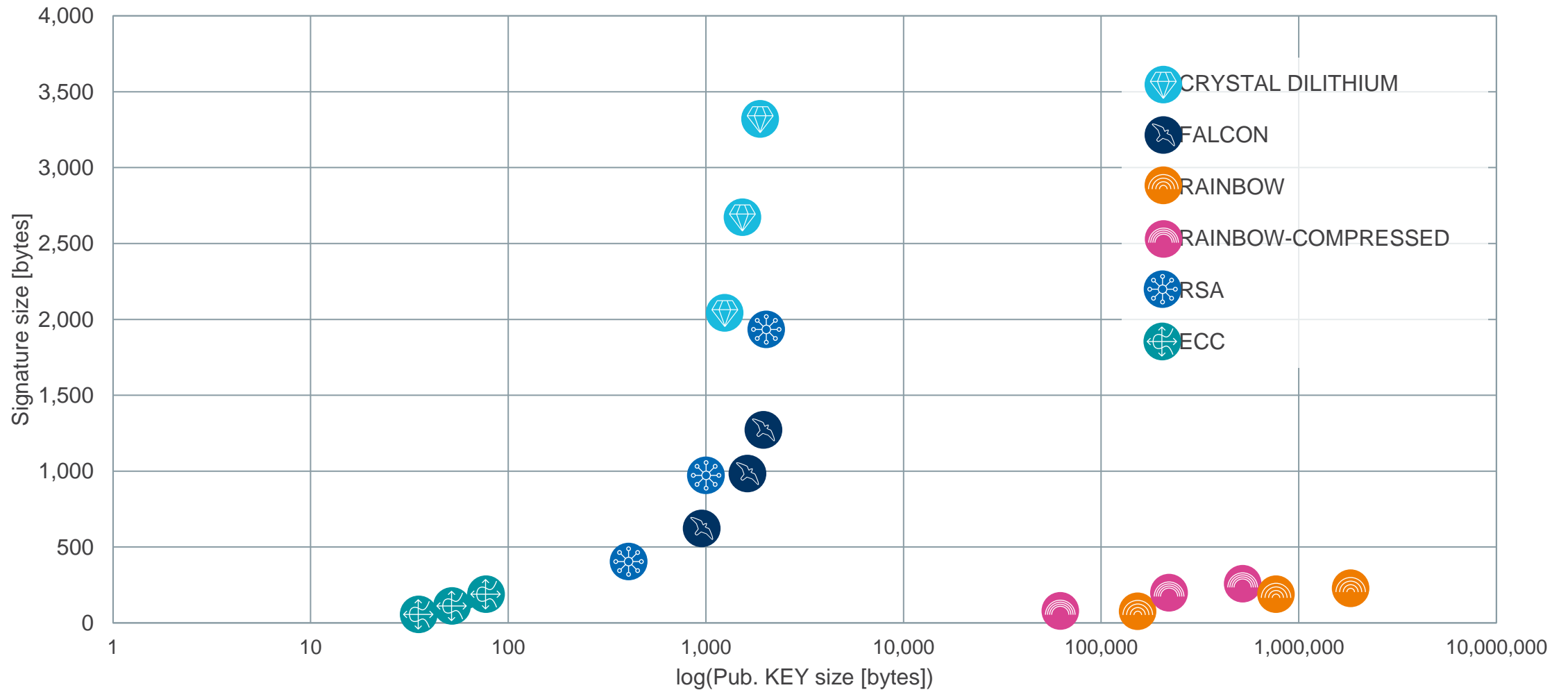
## Standardization of Quantum Safe Cryptography

Quantum Safe Cryptography	Digital Signature	Public-Key Encryption	Key Agreement
Hash-based signatures (e.g. SPHINCS+)	X		
Lattices (e.g. Dilithium, Kyber, NewHope, Frodo)	X	X	X
Error Correcting Codes (e.g. Classic McEliece)	X	X	
Elliptic Curve Isogenies (e.g. SIKE)	X	X	X
Multivariate (e.g. Rainbow)	X	X	

- ◆ Some stateful hash-based signatures are accepted as quantum safe
  - ◆ eXtended Merkle Signature Scheme XMSS
  - ◆ Leighton-Micali Hierarchical Signature System HSS

## The Impacts of Post Quantum Cryptography – e.g. Signature Algorithms

## NIST ROUND 3 – SIGNATURE FINALISTS vs. RSA / ECC



## The Impacts of Post Quantum Cryptography

### ◆ Key size and certificate size

- ◆ Memory capacity of a PIV card / EMV card chip

### ◆ Communication overhead

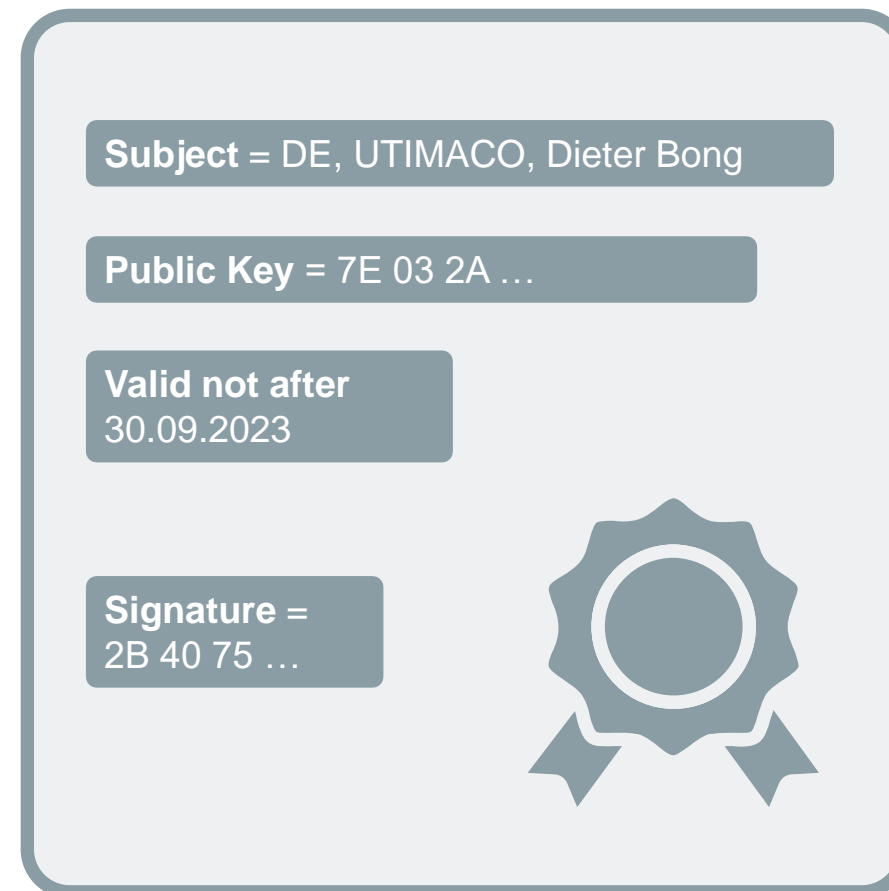
- ◆ Latency

### ◆ Signature creation / verification time

- ◆ Real-time requirements in grid control systems

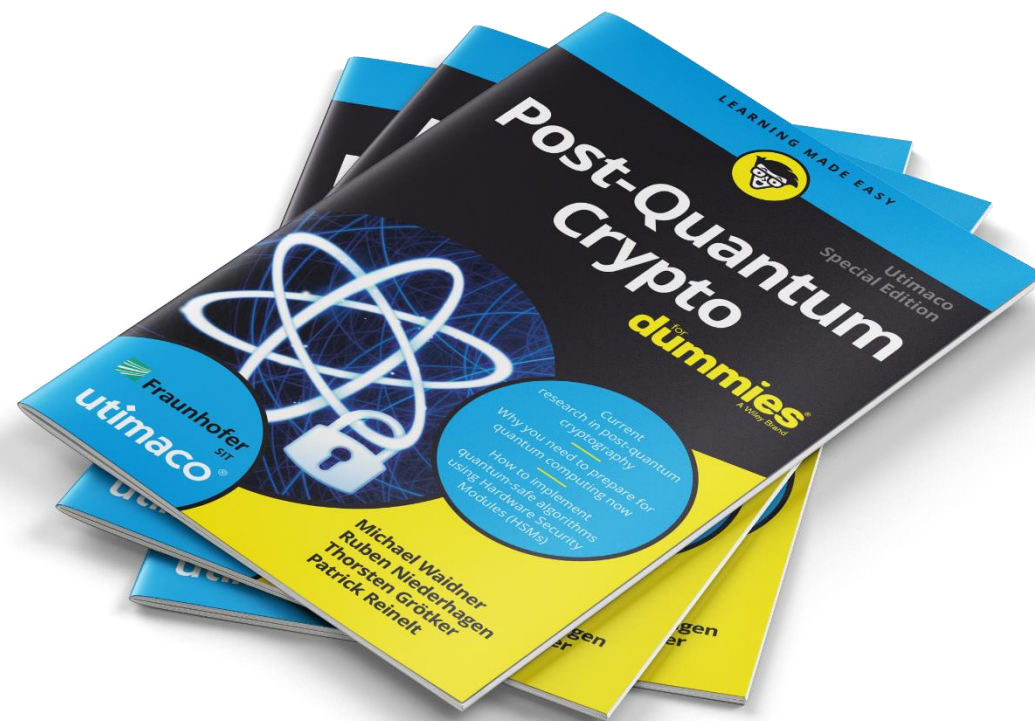
### ◆ Power consumption

- ◆ Battery lifetime of a smart gas meter





Make yourself familiar with Post Quantum Cryptography



- ◆ Know more about PQC
  - ◆ Read Post-Quantum Crypto for dummies
- ◆ Test and evaluate PQC
  - ◆ Download Q-Safe simulator  
<https://support.hsm.utimaco.com/hsm-simulator>



Try for FREE!

Need to implement quantum-safe algorithms?  
Get in touch and try our Q-safe HSM simulator!



## The Road to Mass Adoption of Post Quantum Cryptography







# Thank you for your attention!



## UTIMACO IS GmbH

Germanusstraße 4 Phone +49 241 1696-0  
52080 Aachen Web [hsm.utimaco.com](https://hsm.utimaco.com)  
Germany E-Mail [hsm@utimaco.com](mailto:hsm@utimaco.com)

## UTIMACO Inc.

900 East Hamilton Avenue Phone +1 (844) UTI-MACO  
Campbell, CA-95008 Web <https://hsm.utimaco.com>  
United States of America E-Mail [hsm@utimaco.com](mailto:hsm@utimaco.com)

**utimaco**<sup>®</sup>

Copyright © 2020 – UTIMACO GmbH

UTIMACO<sup>®</sup> is a trademark of UTIMACO GmbH. All other named Trademarks are Trademarks of the particular copyright holder.  
All rights reserved. Specifications are subject to change without notice.