Fraunhofer
SINGAPORE

FRAUNHOFER WORKSHOP SERIES
FWS #01

FRAUNHOFER SINGAPORE
GROUP „CYBER- AND INFORMATION SECURITY“

FRAUNHOFER WORKSHOP ON
POSTQUANTUM CRYPTOGRAPHY IN PRACTICE

HOW TO MAKE IT SMALL, FAST AND SECURE

FRAUNHOFER WORKSHOP SERIES (FWS) are bridging academia and industrial experts to tackle foresighted research into practical solutions. Our FWS events include background lectures, round-tables and hands-on sessions. The goal is to contribute to application-oriented research and to support the transfer of academic research to the industrial domain.

Quantum mechanics has been one of the most important achievements in the field of theoretical physics in the 20th century. In the 21st century, we expect as practical application of this theory, the development of quantum computers. Quantum computers will be able to break important cryptographic primitives used in today's digital communication. Therefore, there are ongoing activities aiming at the development, standardization, and application of post-quantum cryptography, i.e., cryptography that is able to resist attacks by quantum computers.

In this workshop, we will investigate post-quantum primitives targeting the requirements of modern internet applications and resource-restricted embedded hardware architectures used in, e.g., Automotive, Critical Infrastructures and "Industrie 4.0".

The workshop will include several lectures and hands-on sessions to improve existing knowledge in various directions:

- On the way to Quantum Computing. What is quantum computing and why does it break cryptographic primitives?
- Challenges for industry and academia
- Theoretical Background on Post-Quantum Schemes (Code-based, Lattice-based, Hash-based, Multivariate, Supersingular Isogeny)
- Efficient Implementations of PQ for Hardware and Software: Optimization in area, memory, speed and power
- Secure Design of PQ schemes: How to design quantum resistant primitives in practice
- Cryptanalysis vs. physical attacks: Side-channel and fault analysis. on PQ crypto systems

When: 8th February, 2018 **Time:** 09:00am - 4:50pm
Where: Fraunhofer Singapore, NS1-1, Level 5

Register at fraunhofer.sg/fws

For more information please contact fws@fraunhofer.sg

Organizer:
Fraunhofer Singapore
Group „Cyber- and Information Security“

About Fraunhofer:
Fraunhofer is the leading organization for applied research in Germany and Europe. Over 25.000 highly qualified employees are covering all areas of research and make customized services possible. **Fraunhofer Singapore** is the first Fraunhofer subsidiary in Asia, developing solutions and services that help companies and industries stay ahead of the competition.

FRAUNHOFER WORKSHOP SERIES
FWS #01

POSTQUANTUM CRYPTOGRAPHY IN PRACTICE
How To Make It Small, Fast and Secure

WORKSHOP PROGRAM

09:00 - 09:10	**Welcome & Introduction** Speaker: Michael Kasper, Fraunhofer Singapore
09:10 - 10:10	**The Power of Quantum Information and Its Applications** Speaker: Prof. Dr. Gu Mile, School of Physical and Mathematical Sciences (SPMS), Nanyang Technological University (NTU), Singapore
10:10 - 11:10	**Introduction to Post-Quantum Cryptography and Major Challenges for the Adoption** Speaker: Dr. Ruben Niederhagen, Fraunhofer SIT, Darmstadt, Germany
11:10 - 11:40	Coffee Break
11:40 - 12:10	**Efficient Code-based Cryptography for FPGAs** Speaker: Dr. Ruben Niederhagen, Fraunhofer SIT, Darmstadt, Germany
12:10 - 12:40	**Side-Channel Attacks on Code-based Cryptography** Speaker: Dr. Bernhard Jungk, Fraunhofer Singapore
12:40 - 13:40	Lunch & Networking
13:40 - 14:40	**Quantum Cryptanalysis: How to Break Some Classical Cryptosystems with Quantum Computers?** Speaker: Prof. Dr. Miklos Santha, CNRS, Univ. Paris Diderot, France, Centre for Quantum Technologies (CQT), National University of Singapore (NUS), Singapore
14:40 - 15:10	**Practical Lattice-Based Cryptography** Speaker: Prof. Dr. Divesh Aggarwal, Department of Computer Science, Centre for Quantum Technologies (CQT), National University of Singapore (NUS), Singapore
15:10 - 15:40	Coffee Break
15:40 - 16:10	**Hash-based Cryptography - IETF CFRG proposal XMSS** Speaker: Dr. Bernhard Jungk, Fraunhofer Singapore
16:10 - 16:40	**Long-term Security Challenges Ahead of Automotive Applications: An Industrial Perspective** Speaker: Dr. Marc Stöttinger, Continental Teves AG, Frankfurt, Germany

When: 8th February, 2018 **Time:** 09:00am - 4:50pm
Where: Fraunhofer Singapore, NS1-1, Level 5

Register at fraunhofer.sg/fws

For more information please contact fws@fraunhofer.sg

Organizer:
Fraunhofer Singapore
Group „Cyber- and Information Security"

About Fraunhofer:
Fraunhofer is the leading organization for applied research in Germany and Europe. Over 25.000 highly qualified employees are covering all areas of research and make customized services possible. **Fraunhofer Singapore** is the first Fraunhofer subsidiary in Asia, developing solutions and services that help companies and industries stay ahead of the competition.