Press Release

Ready for tomorrow: Infineon demonstrates first post-quantum cryptography on a contactless security chip

Munich, Germany – 30 May 2017 – Due to their computing power, quantum computers have the disruptive potential to break various currently used encryption algorithms. Infineon Technologies AG (FSE: IFX / OTCQX: IFNNY), the leading provider of security solutions, is ready to provide a smooth transition from today's security protocols to next-generation post-quantum cryptography (PQC). The company has now successfully demonstrated the first PQC implementation on a commercially available contactless security chip, as used for electronic ID documents. This places Infineon in the pioneering position for encryption that withstands quantum computing power.

"Demonstrating post-quantum cryptography on a contactless security chip puts Infineon in a leading position in this field," said Stefan Hofschen, President of the Chip Card & Security Division of Infineon. "Our security solutions rely on trusted and standardized private and public key algorithms. To better respond to security threats that are yet to come, we continuously collaborate with the academic community, customers and partners. And we push for future standards that can be executed efficiently and securely on small and embedded devices."

Quantum computer attacks on today's cryptography are expected to become reality within the next 15 to 20 years. Once available, quantum computers could solve certain calculations much faster than today's computers, threatening even best currently known security algorithms such as RSA and ECC. Various internet standards like Transport Layer Security (TLS), S/MIME or PGP/GPG use cryptography based on RSA or ECC to protect data communication with smart cards, computers, servers or industrial control systems. Online banking on "https" sites or "instant messaging" encryption on mobile phones are well-known examples.

For the Business and Trade Press: INFCCS201705.056e

Media Relations:	**Name:**	**Phone:**	**Email:**
Worldwide Headquarters	**Karin Braeckle**	+49 89 234 23424	karin.braeckle@infineon.com
U.S.A.	**Sian Cummings**	+1 310 252 7148	sian.cummings@infineon.com
Asia	**Chi Kang David Ong**	+65 6876 3070	david.ong@infineon.com
Japan	**Yoko Sasaki**	+81 3 5745 7340	yoko.sasaki@infineon.com
Investor Relations	**EU/APAC/USA/CAN**	+49 89 234 26655	investor.relations@infineon.com

Chip memory size and computation time are key

Security experts at Infineon's Munich headquarters and the Center of Excellence for contactless technologies in Graz, Austria, made a breakthrough in this field. They implemented a post-quantum key exchange scheme on a commercially available contactless smart card chip. Key exchange schemes are used to establish an encrypted channel between two parties. The deployed algorithm is a variant of "New Hope", a quantum-resistant cryptosystem also explored successfully by Google on a development version of the Chrome browser.

"The phantom of the quantum computer is keeping academia and the IT industry on high alert," said Thomas Pöppelmann from Infineon's Chip Card & Security Division, who has been co-developing the New Hope algorithm. "At Infineon, we are proud to be the first to transfer PQC onto contactless smart cards. Our challenges comprised the small chip size and limited memory capacity to store and execute such a complex algorithm as well as the transaction speed." Thomas Pöppelmann and his co-researchers received the prestigious Facebook Internet Defense Prize 2016 for the development of New Hope.

In a world of quantum computers, PQC should provide a level of security that is comparable with what RSA and ECC provide today in the classical computing world. However, to withstand quantum calculation power, key lengths need to be longer than the usual 2048 bits of RSA or the 256 bits of ECC. Nevertheless, the researchers at Infineon were able to implement New Hope on a commercially available security chip without requiring additional memory space and hence a larger chip size.

Standardization bodies are expected to agree on one or multiple PQC algorithms within the next few years before governments and industries mandate the migration. Infineon is actively participating in the development and standardization process in order to enable a smooth transition and to address security challenges that may arise in the advent of quantum computers.

About quantum computers

A quantum computer uses "qubits" that can exist in any superposition rather than bits (0 or 1) in a conventional device. Consequently, certain calculations can be performed simultaneously and far faster than ever before, solving problems that

For the Business and Trade Press: INFCCS201705.056e

Media Relations:	**Name:**	**Phone:**	**Email:**
Worldwide Headquarters	**Karin Braeckle**	+49 89 234 23424	karin.braeckle@infineon.com
U.S.A.	**Sian Cummings**	+1 310 252 7148	sian.cummings@infineon.com
Asia	**Chi Kang David Ong**	+65 6876 3070	david.ong@infineon.com
Japan	**Yoko Sasaki**	+81 3 5745 7340	yoko.sasaki@infineon.com
Investor Relations	**EU/APAC/USA/CAN**	+49 89 234 26655	investor.relations@infineon.com

would require unattainable amounts of conventional computing power today. With operations that are thousands of times faster, quantum computers offer new possibilities, for instance, for searching large databases, for chemical or physical simulations, and in material design, etc. However, this operating power may also allow the decoding of currently used encryption algorithms that are practically impossible to decode with technologies available today.

About Infineon

Infineon Technologies AG is a world leader in semiconductor solutions that make life easier, safer and greener. Microelectronics from Infineon is the key to a better future. In the 2016 fiscal year (ending September 30), the company reported sales of about 6.5 billion euros with more than 36,000 employees worldwide. Infineon is listed on the Frankfurt Stock Exchange (ticker symbol: IFX) and in the USA on the over-the-counter market OTCQX International Premier (ticker symbol: IFNNY).

Further information is available at www.infineon.com
This press release is available online at www.infineon.com/press

Follow us:
twitter.com/Infineon - facebook.com/Infineon – linkedin.com/infineon

For the Business and Trade Press: INFCCS201705.056e

Media Relations:	**Name:**	**Phone:**	**Email:**
Worldwide Headquarters	**Karin Braeckle**	+49 89 234 23424	karin.braeckle@infineon.com
U.S.A.	**Sian Cummings**	+1 310 252 7148	sian.cummings@infineon.com
Asia	**Chi Kang David Ong**	+65 6876 3070	david.ong@infineon.com
Japan	**Yoko Sasaki**	+81 3 5745 7340	yoko.sasaki@infineon.com
Investor Relations	**EU/APAC/USA/CAN**	+49 89 234 26655	investor.relations@infineon.com