NEWS AND INSIGHTS FROM THE WORLD OF ID SECURITY

AUGUST 2020 | #26

The VAULT

BRAVE NEW WORLD

FEATURED ARTICLE

The reason why secure biometric systems still require hardware based security

Infineon Technologies

ALSO IN THIS ISSUE

Contents

Imprint

THE VAULT
Published bi-annually by Krowne Communications GmbH, Berlin.
PUBLISHER: Krowne Communications GmbH, Steve Atkins, Kurfürstendamm 194, 10629 Berlin
EDITOR-IN-CHIEF: Steve Atkins
ART DIRECTOR: Lana Petersen
PARTNER DIRECTOR: Yvonne Runge
EDITORIAL CONTRIBUTIONS: Rainer Bergmann, Daniela Previtali, Bernd Zwattendorfer, Maurizio Skerlj, Markus Mosenbacher, Alexander Sipua Ngnobamdjum, Markus Hoffmeister, Uljana Belokrinicka, Dr. Mike Bergmann, Carmen Kempka
PHOTOS: WIBU SYSTEMS, INFINEON TECHNOLOGIES, ISTOCKPHOTO, MÜHLBAUER ID SERVICES, CRYPTOVISION, X INFOTECH, KROWNE COMMUNICATIONS, SIPUA CONSULTING
PRINTING: DRUCKEREI HÄUSER KG, COLOGNE

⟨PQC|4|MED⟩ *Crypto-agility* for post-quantum SECURITY in *medical DEVICES*

Dr. Carmen Kempka, Senior Cryptography Expert, Wibu-Systems

Each hardware generation brings new potential, and with it, new ways to attack the integrity and confidentiality of sensitive data. Progress in the field of quantum computers is particularly critical: A sufficiently powerful quantum computer could completely break a large part of the cryptographic methods currently in use and carry out known attacks much more efficiently than conventional computers. In order to be able to guarantee long-term security, it is important to always be one step ahead of the curve and to prepare now for the potential threats brought by the hardware of the future.

PQC4MED is a research project funded by the German Ministry of Education and Research (BMBF), started at the end of 2019, and dedicated to equipping medical devices with post quantum cryptography (PQC) capabilities. As a project coordinator, Wibu-Systems is cooperating with partners from science and industry, to prepare medical devices for the coming post-quantum era through security-by-design. The primary goal of this project is for the medical technology sector to integrate crypto-agility in embedded systems early on in the manufacturing process. Secure elements play an important role in this process, as they can support the flexible substitution of cryptographic algorithms. Algorithms can be replaced in secure elements either "in field" by means of firmware updates or "in factory" by adopting modular hardware. This approach keeps a window open for introducing future algorithms that are resistant against quantum computers, but whose security and robustness are still being investigated. The update process itself must also be protected, especially for "in field" updates, to be able to react robustly to new threats.

Wibu-Systems intends to lay down a new foundation for the production of PQC-capable systems, with a sustainable secure infrastructure and a platform for highly secure updates.

Our Partners

In PQC4MED, we are bundling the competencies of our partners from science and industry. Infineon Technologies AG has already contributed significantly to SPHINCS+ and NewHope, candidates for NIST standardization for post-quantum algorithms. In this project, Infineon is working on long-term security for firmware updates and generic hardware modules for the secure elements planned to run the post-quantum secure algorithms. Schölly Fiberoptic GmbH is implementing and testing lastingly secure update mechanisms for the firmware of secure elements, as well as for software and data protection on endoscopy devices. macio GmbH is supporting PQC4MED with modular software libraries and interfaces for communication between applications and post-quantum secure protectors. The Institute for IT Security (ITS) of the University of Luebeck, Germany is analyzing post-quantum algorithms with a focus on side-channel analysis in software and hardware. The German Research Center for Artificial Intelligence (DFKI) in Bremen, Germany is implementing, integrating, and evaluating post-quantum algorithms for use in medical devices, concentrating on their hardware implementation and evaluation in practice. The research group KASTEL, as part of the Institute for Theoretical Computer Science (ITI) of the Karlsruhe Institute of Technology (KIT), will model and analyze the security of update mechanisms in the search for a verifiably secure update mechanism. Finally, Wibu-Systems AG is contributing its unique expertise and experience with using hardware secure elements as part of a holistic and comprehensive protection and licensing infrastructure.

Crypto-agility: Flexibility is key

Cryptography that is secure against attacks from quantum computers, as well as the mathematical problems it is based on, have received much less investigative attention from researchers than conventional cryptography. By contrast, the problem of factorizing large numbers, on which the RSA cryptosystem is based, was originally introduced by Euclid around 2300 years ago.

This project calls for intensive attention to current progress in the field of post-quantum security and its standardization. At the same time, our update platform and secure elements must be equipped with the necessary crypto-agility to be able to react to new results in the field of post-quantum cryptography if they want to guarantee lasting security.

PQC in the medical field: A special challenge

Medical technology is a market known for its heavy reliance on embedded systems. At the same time, this raises the legal bar considerably in terms of the German Data Protection Ordinance's and EU-GDPR's standards for the trustworthiness, long-term security, and integrity of personal data during processing, transmission, and storage.

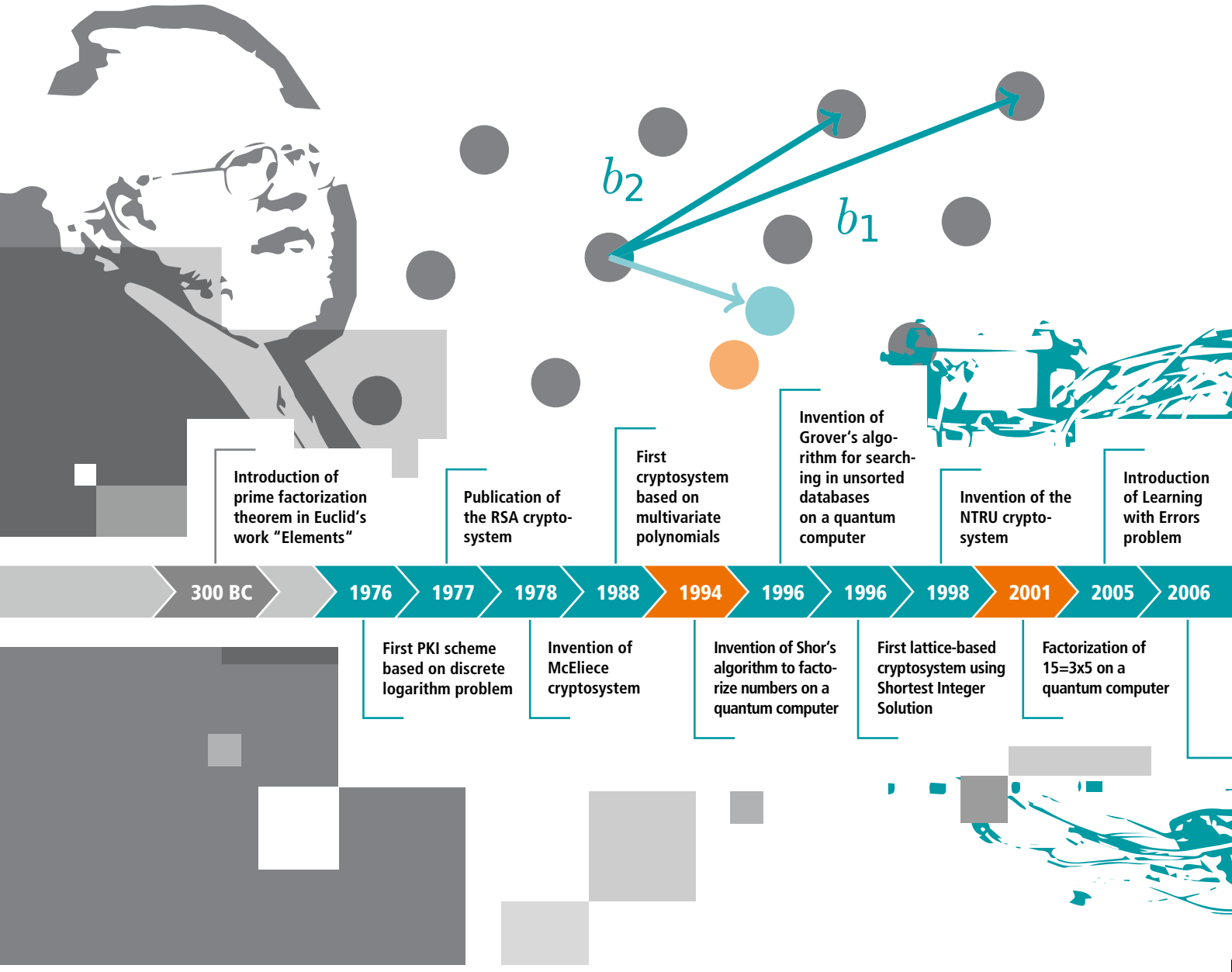
Despite the often lower memory capacity and computing power of embedded systems, the high security requirements for medical devices must be met, and both highly sensitive patient data and the intellectual property of the often extremely complex software on medical devices must be protected in the best possible way.

Is conventional cryptography really threatened by quantum computers?

Many of the common encryption, signature, and key exchange methods are based on hard mathematical problems that cannot be solved with currently available algorithms with the ease or speed needed in actual practice to crack the encryption. For example, RSA encryption is based on the problem of factorizing large numbers, while cryptographic algorithms such as DSA, ECIES, ECDSA and ECDH are based on discrete logarithms. These are just some of the cryptographic algorithms genuinely threatened by quantum computing.

In 1994, Peter Shor first developed an algorithm that can efficiently factorize large numbers using a quantum computer. This algorithm can be extended to calculate discrete logarithms, even on elliptic curves. In 1996, Lov Grover developed a quantum algorithm that efficiently finds elements in an unsorted database, also endangering symmetric cryptography.

The mentioned asymmetric cryptographic algorithms based on factorization or discrete logarithms would be broken by a sufficiently strong quantum computer. For most of the commonly used symmetric schemes and hash algorithms, the key length or output length would have to be at least doubled in order to achieve a similar level of security as they had without the availability of quantum computers.



How acute is the danger of quantum computers?

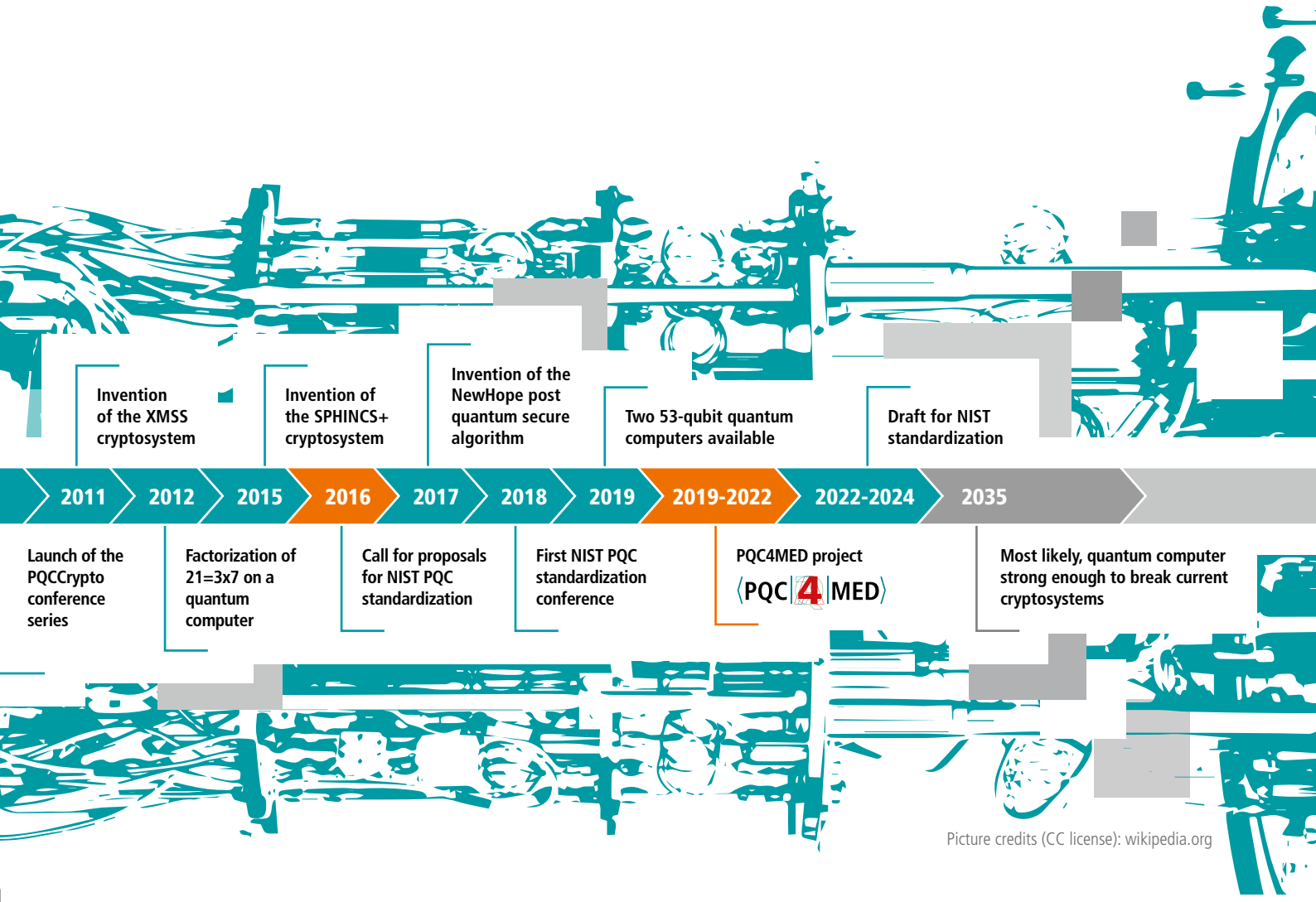
When Shor and Grover published their algorithms, quantum computers were still a theoretical construct, with their actual reality seemingly far away. Then, in 2001, the first number was factorized on a working quantum computer: 15 = 3 x 5.

Today, quantum computers with more than 50 qubits exist. Both IBM and Google have already built a 53-qubit quantum computer, and several other companies are actively researching the construction of quantum computers of different architectures. Programming languages for quantum computers have already been developed.

However, this does not yet represent an acute danger for the cryptographic procedures currently in use. In order to break RSA 2048 by factorization, a few thousand qubits would be necessary even on an ideal, error-free quantum computer. However, due to the error-proneness and short lifespan of quantum states, one would actually need a few million qubits. Breaking discrete logarithm-based methods such as ECDSA would be a challenge of a similar order of magnitude.

At what point do we have to start worrying?

A very simple estimate is provided by Mosca's Theorem: "If X + Y > Z, then worry"



Picture credits (CC license): wikipedia.org

Here, X is the time for which our currently used cryptography has to remain safe. Y is the time needed to prepare our infrastructure for switching its cryptographic paradigm, substituting the corresponding procedures, and re-protecting all data currently protected with previous procedures. Z is the time it takes until a quantum computer is available that is powerful enough to break current cryptographic procedures. According to the NIST PQC project, this could be as soon as Z=15 years.

Expert groups and standardization committees are currently working intensively on post-quantum security. The selection of candidates for NIST standardization is already in its second round, and a draft for the standardization of post-quantum-secure methods is planned for 2022-2024.

It is difficult to predict when exactly a quantum computer will exist that can break current cryptography. It is important, however, that the move to post-quantum-secure procedures takes place before this happens. Our infrastructure must already be adapted to PQC by then, and sensitive data must already be protected with procedures that are robust against quantum computers.

How does post-quantum cryptography work?

Like most cryptography used so far, post-quantum secure methods are based on hard mathematical problems, for which neither a conventional nor an efficient quantum algorithm has yet been found.

WIBU SYSTEMS

CodeMeter – the Catalyst of the IoT driven Economy

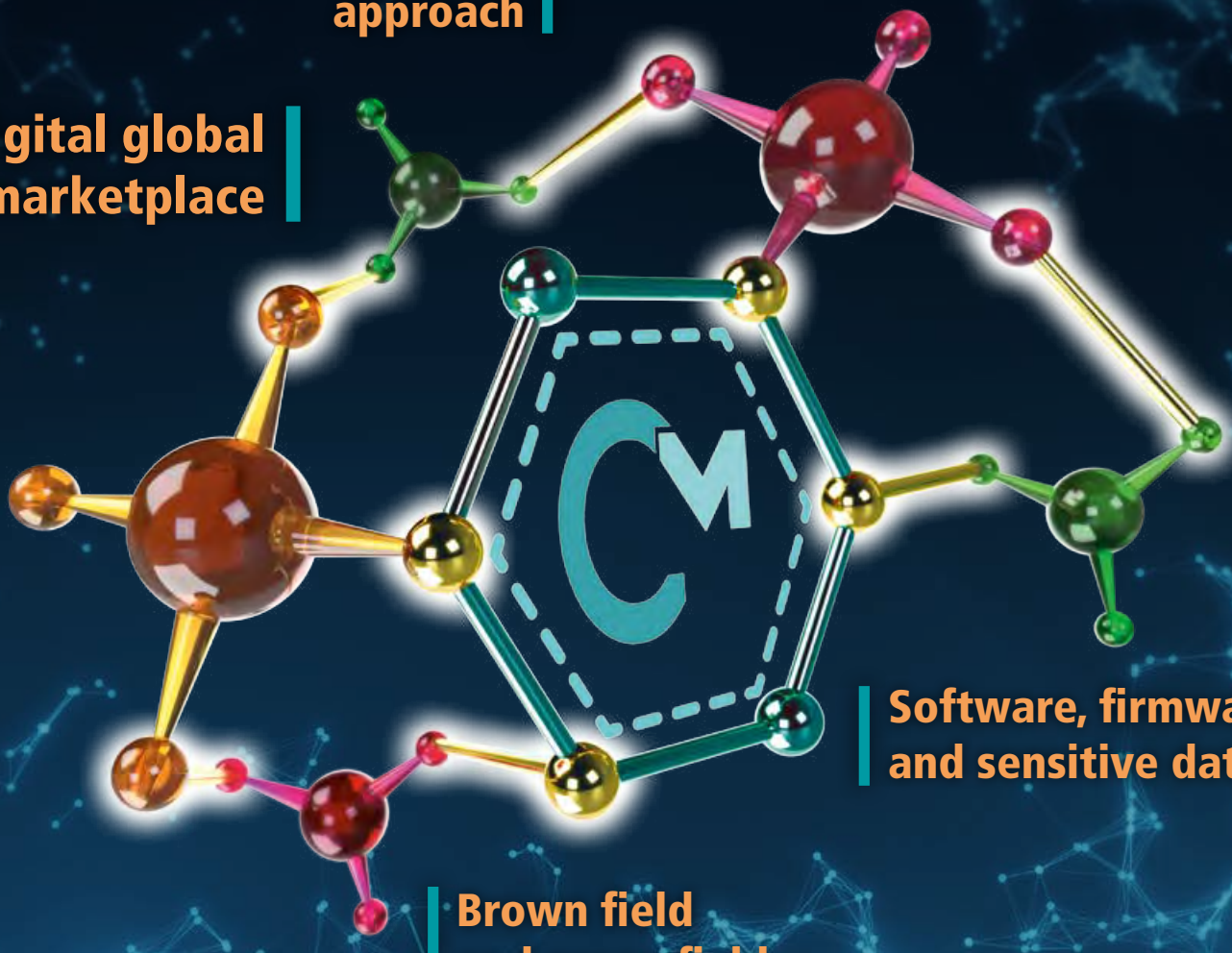
Let CodeMeter inspire you with new license-driven business models

- Protect your digital assets from piracy and reverse engineering
- Secure the integrity of your endpoints from tampering
- Implement license-based readily adaptable business models

From the cloud down to FPGAs

Customer centric approach

Digital global marketplace



Software, firmware, and sensitive data

Brown field and green field

Don't wait any longer
Start protecting your IP now!
s.wibu.com/sdk-cm

+49 721 931720
sales@wibu.com
www.wibu.com

SECURITY
LICENSING
PERFECTION IN PROTECTION