

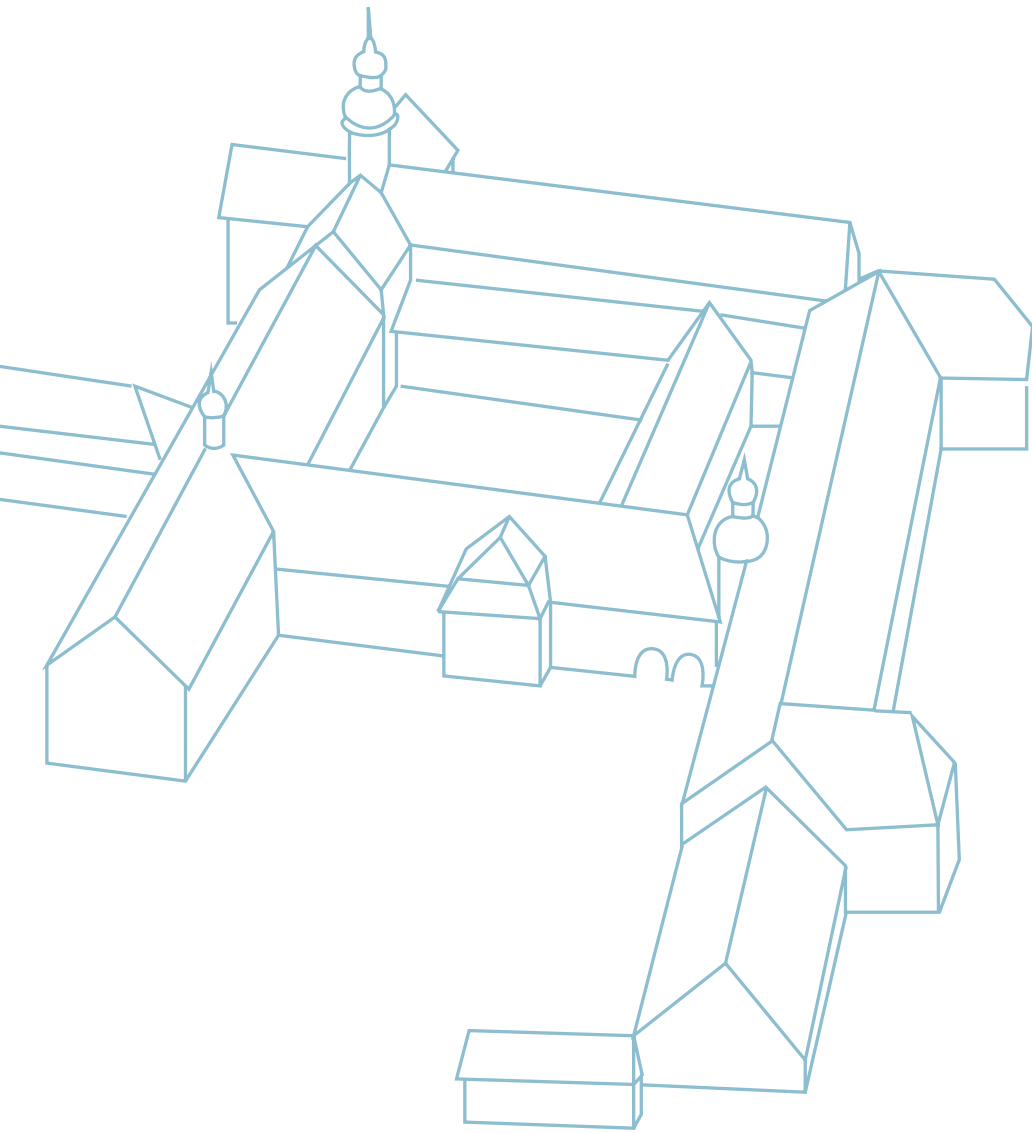
EBERBACHER GESPRÄCH ON »NEXT GENERATION CRYPTO«

01/2018

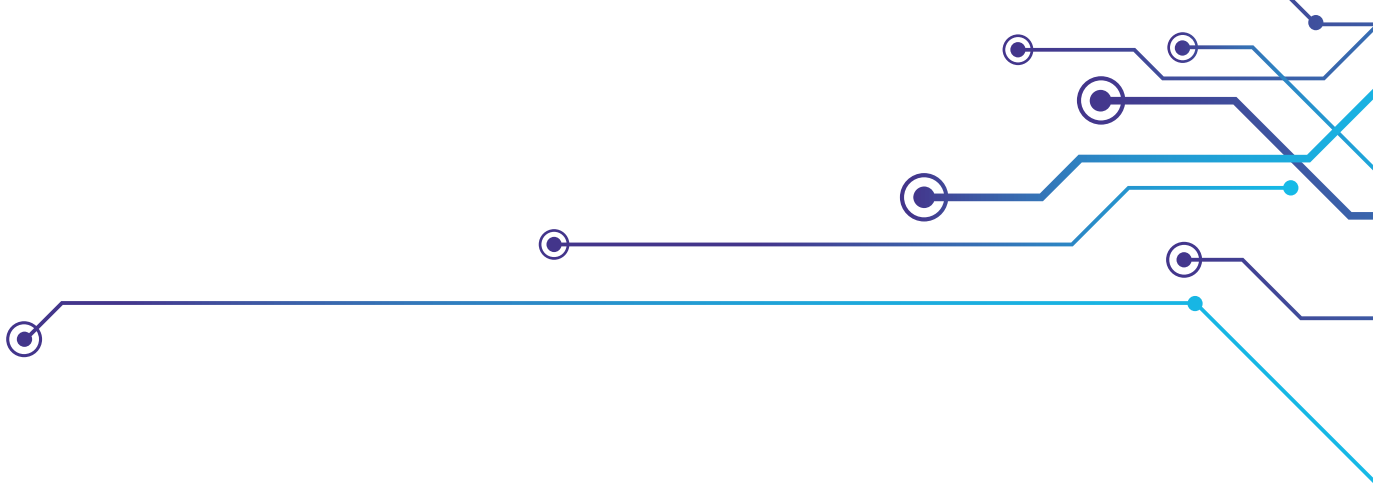
Eberbacher
Gespräche



$\varphi(n) = (p-1)(q-1)$
 $\text{ggT}(e, \varphi(n)) = 1$
 $d \cdot e \equiv 1 \pmod{\varphi(n)}$
 $c = m^e \pmod{n}$
 $m = c^d \pmod{n}$



PREAMBLE



Applied research on IT security requires a dialogue between science and enterprises to obtain application relevant responses to fundamental questions such as: What are the current challenges for IT security and privacy protection? What is to be expected in the future? What can and shall technology achieve? Where are the limits of what is technically feasible? Where are new ideas necessary?

The »Eberbacher Gespräche« organized by Fraunhofer SIT provide a forum for such a dialogue. Experts from commerce, administration and the scientific community meet at Kloster Eberbach in Rheingau for one day to find answers to questions like these, relating to specific topics. In May 2017, the topic was »Next Generation Cryptography«.

This paper summarizes the results of this dialogue but does not necessarily reflect the views of the participants' companies.

Participants:

Christian Flory (Hessen-IT, Hessen Trade & Invest GmbH)

Michael Herfert (Fraunhofer SIT)

Marcus Janke (Infineon technologies AG)

Dr. Vangelis Karatsiolis (MTG AG)

Axel Krein (AIRBUS Deutschland GmbH)

Dr. Michael Kreutzer (Fraunhofer SIT)

Dr. Ruben Niederhagen (Fraunhofer SIT)

Dr. Markus Rückert (European Space Agency (ESA))

Dr. Harald Schöning (Software AG)

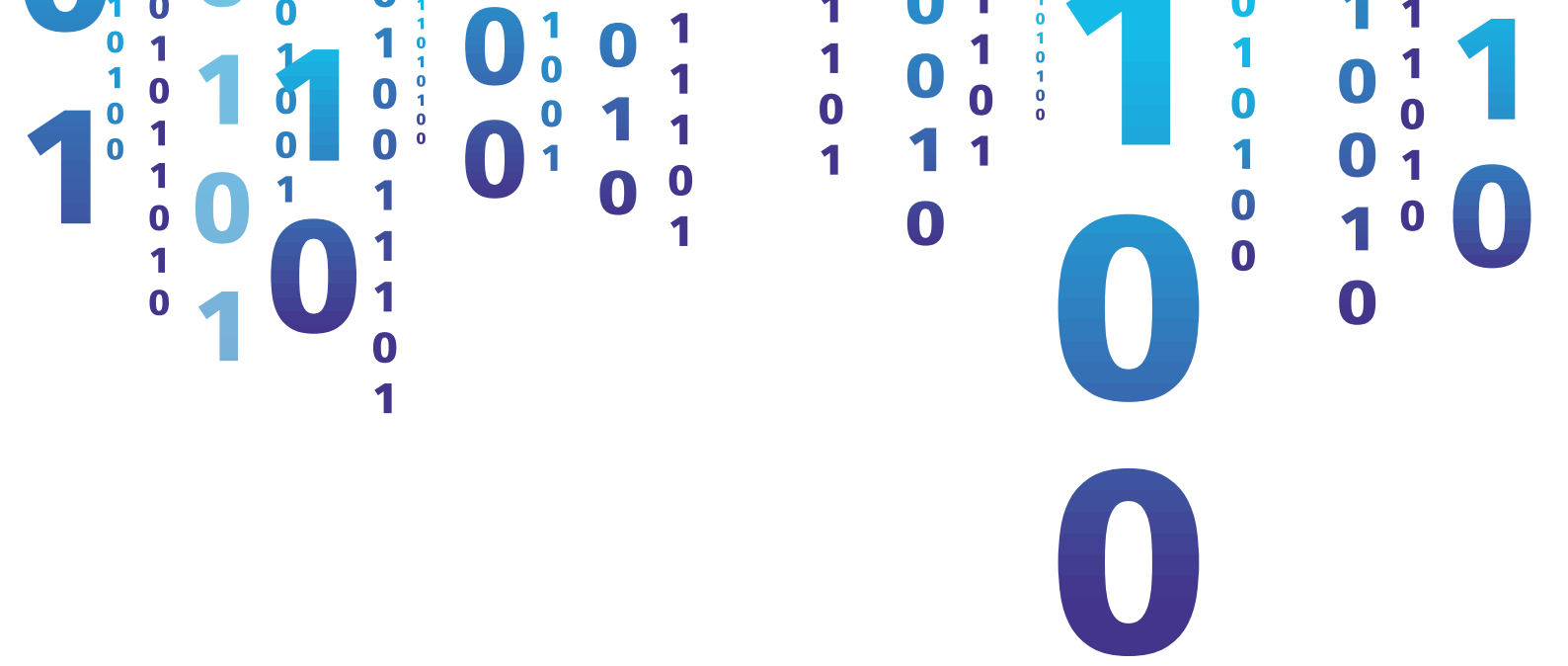
Bert Skaletski (Merck KGaA)

Dr. Dirk Stegemann (Robert Bosch GmbH)

Dr. Marc Stöttinger (Continental)

Dr. Falko Strenzke (cryptosource GmbH)

Prof. Dr. Michael Waidner (Fraunhofer SIT)



00

- 5.1 Public Awareness and Understanding of Cryptography
- 5.2 EU-Standards for Cryptography
- 5.3 Funding for Applied and Interdisciplinary Cryptographic Research
- 5.4 Council of Crypto Sages
- 5.5 Cookbook for Cryptographic Solutions
- 5.6 Minimal Requirements for Cryptographic Solutions
- 5.7 Inventory of Cryptographic Functions

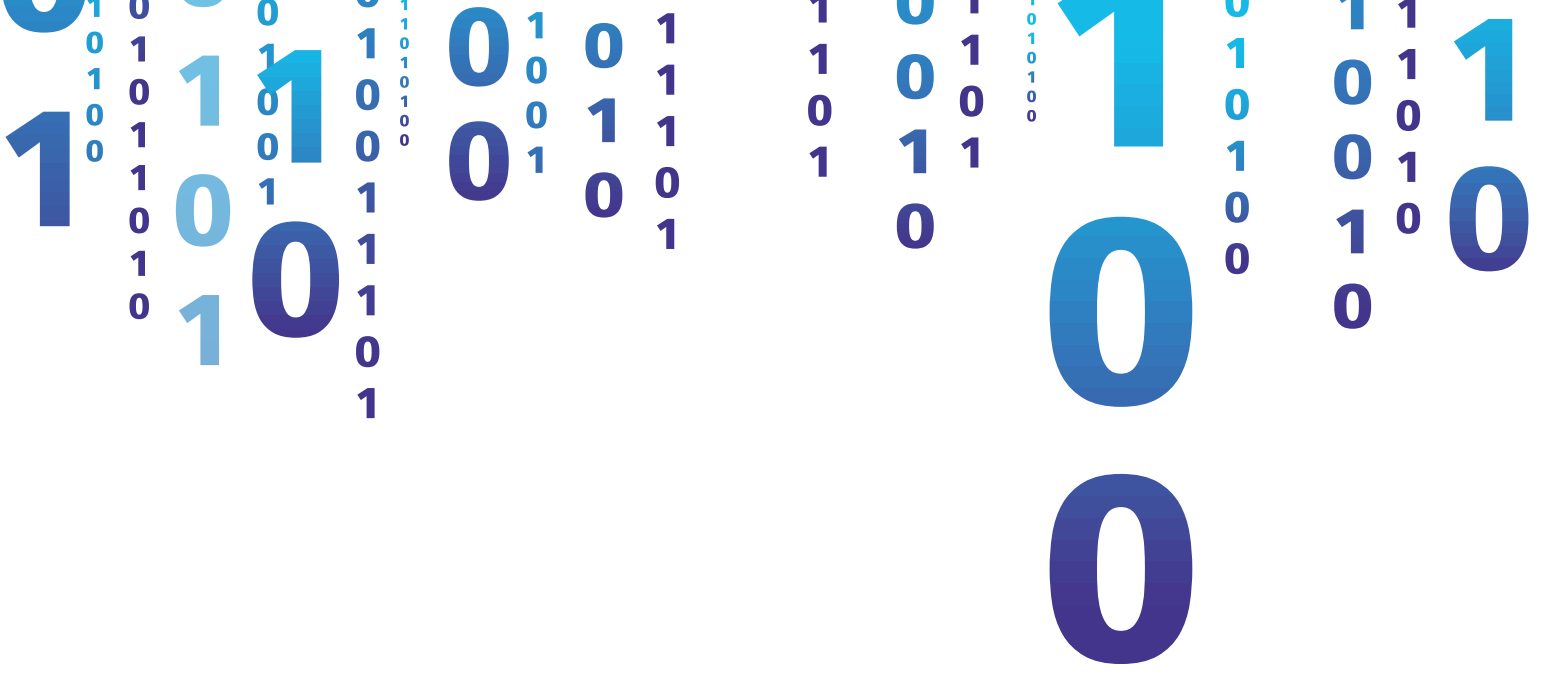
To policy makers on federal, and state levels	X		X		X		
To policy makers on EU levels	X	X	X	X	X	X	
To industry		X	X		X	X	X
To institutions of applied research			X		X	X	

1. SUMMARY

Online banking, blockchain technology, and security mechanisms for the Internet of Things all rely on cryptography. The secure transmission of confidential data (e.g., credit card numbers, tax declarations, state secrets) over insecure channels (e.g., telephony, Internet) would be impossible without cryptography. Companies are using cryptography for protecting their own confidential data and IT systems, and for providing secure services and solutions to customers and consumers. However, industry and attackers attempting to break cryptographic keys, primitives, protocols or implementations are caught in an arms race. Therefore, systems that are using cryptography need to be maintained and patched in order to resist the increasing power of attackers, and industry must be prepared for the transition to the next generation of cryptography whenever established primitives or parameters are at risk of not being secure any longer. Just the more so as the technological development of quantum computers is posing a severe threat to many cryptographic primitives.

In order to discuss the challenges that industry is facing in the described transition process, Fraunhofer Institute for Secure Information Technology SIT conducted an “Eberbacher Gespräch” on May 23rd 2017 on the topic “Next Generation Cryptography”. At this event, participants from industry, science and the public sector identified key challenges for three groups of industry differently involved in cryptography: industry that is using cryptography in their everyday processes; industry that is integrating off-the-shelf cryptography into their products; and industry that is implementing cryptography in order to offer off-the-shelf solutions. The participants jointly propose seven recommendations in order to simplify the usage of cryptography and to support the transition to next generation cryptography:

1. Improvement of public awareness and understanding of basic cryptography
2. EU-standards for cryptography that create trust in cryptographic systems
3. Significant funding for applied and interdisciplinary cryptographic research to secure fast progress in crypto agility
4. A Council of Crypto Sages that develops recommendations and provides counsel to policy makers on questions of standardisation and technology development
5. A Cookbook for Cryptographic Solutions that helps industry to produce secure cryptographic solutions efficiently
6. Minimal requirements for cryptographic solutions that improve business security
7. Analysis of cryptographic inventory to reduce response time in case of a security incident or cryptographic lapse



Bit

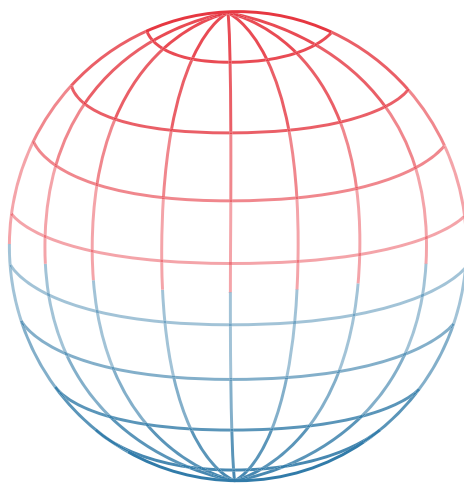
0



1

Qubit

0



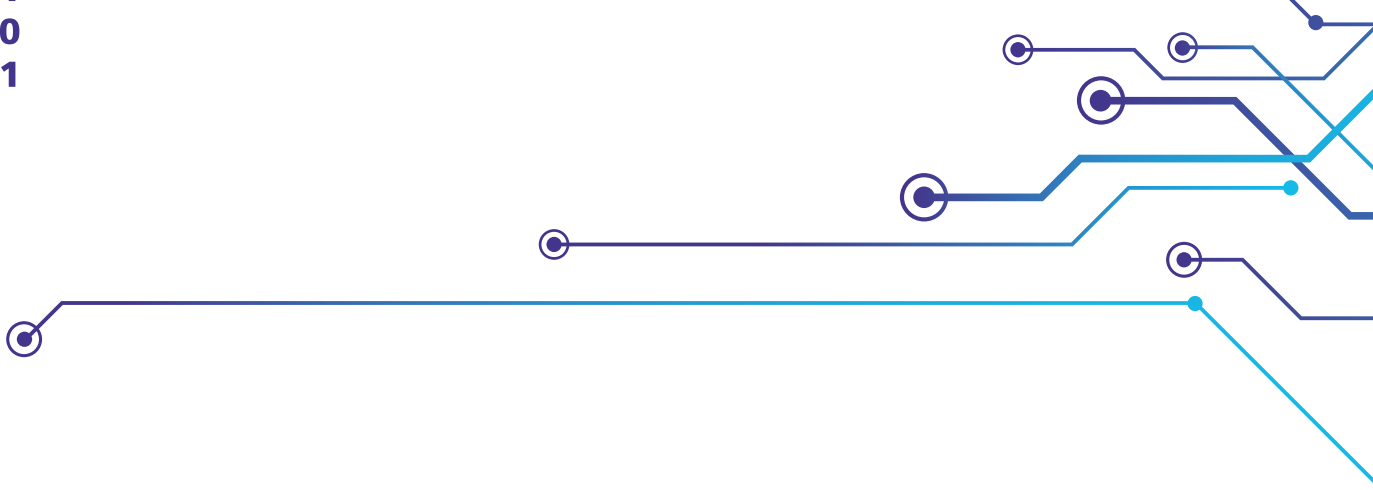
1

Definition (MIT Technology Review)

“At the heart of quantum computing is the quantum bit, or qubit, a basic unit of information analogous to the 0s and 1s represented by transistors in your computer. Qubits have much more power than classical bits because of two unique properties: they can represent both 1 and 0 at the same time, and they can affect other qubits via a phenomenon known as quantum entanglement. That lets quantum computers take shortcuts to the right answers in certain types of calculations.”

2. INTRODUCTION

1 0 0
0 1 1
0 0 0



Cryptography is a crucial building block for achieving IT security in the modern, connected world. However, the security of almost all cryptographical schemes are not static but are connected to technological advancement. More and more computational power is available to an attacker and better attacks on cryptographic schemes are being developed. Also new technologies like quantum computers pose a threat to well-established cryptography. Due to these developments, processes and products that rely on cryptography to achieve security must be versatile and be able to adapt to changing conditions.

2.1 EROSION OF CRYPTOGRAPHIC PRIMITIVES AND PARAMETERS

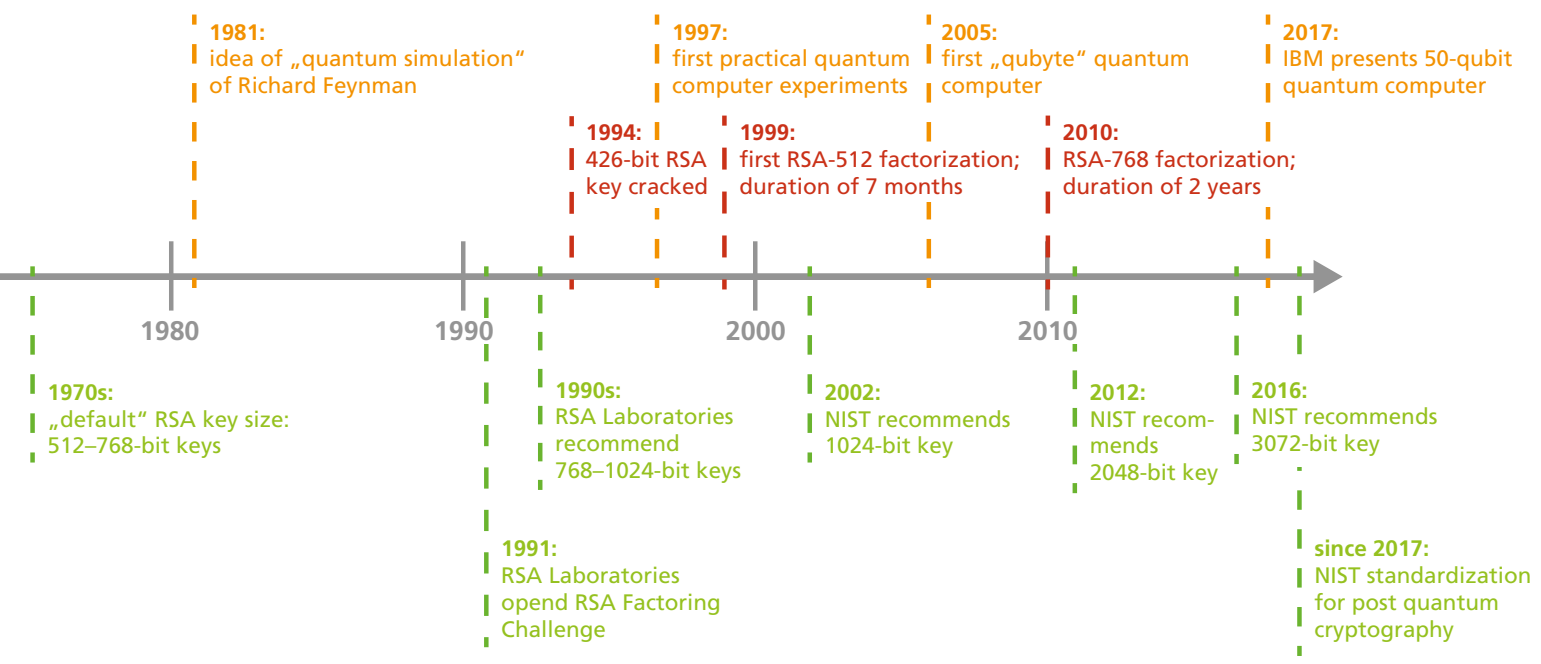
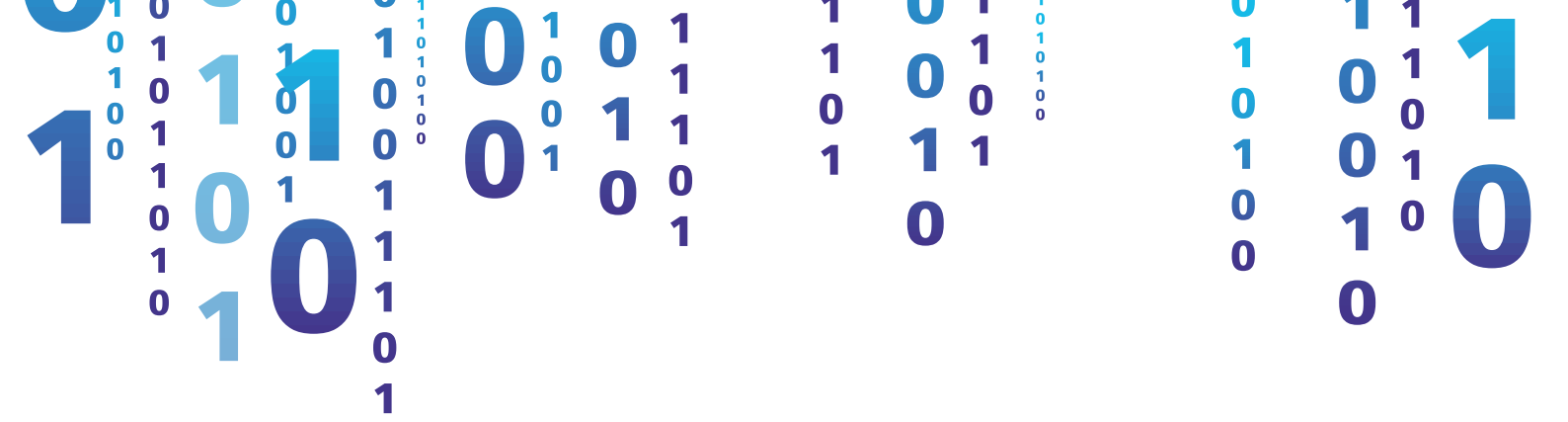
Practically all cryptography used today is based on computational complexity. This means that it is in theory possible to break any such encryption, but that an attacker needs a tremendous amount of computational power and an infeasible amount of time. For example, an attacker who attempts to break an AES-128 encryption by testing all possible keys using the largest public supercomputer available today requires at least 5×10^{21} seconds which is about 12,000 times the age of the universe.

However, in the past there have been many cases where cryptographic primitives and parameters were broken due to improvements in computational power. For example, when the National Institute of Standards and Technology (NIST, at the time still called "National Bureau of Standards") of the USA introduced the Data Encryption Standard (DES) in the 1970s, the cost of breaking DES by performing up to $2^{56} = 72,057,594,037,927,936$ individual DES encryptions seemed infeasible. Today, using specialized hardware, breaking one DES key takes less than one day. Due to its computational weakness, NIST deprecated and removed DES from its standards in the late 1990s and the early 2000s and replaced it with the robust and as of today secure Advanced Encryption Standard (AES) mentioned above. Nevertheless, even today many legacy systems and applications are using or at least are supporting the vulnerable DES.

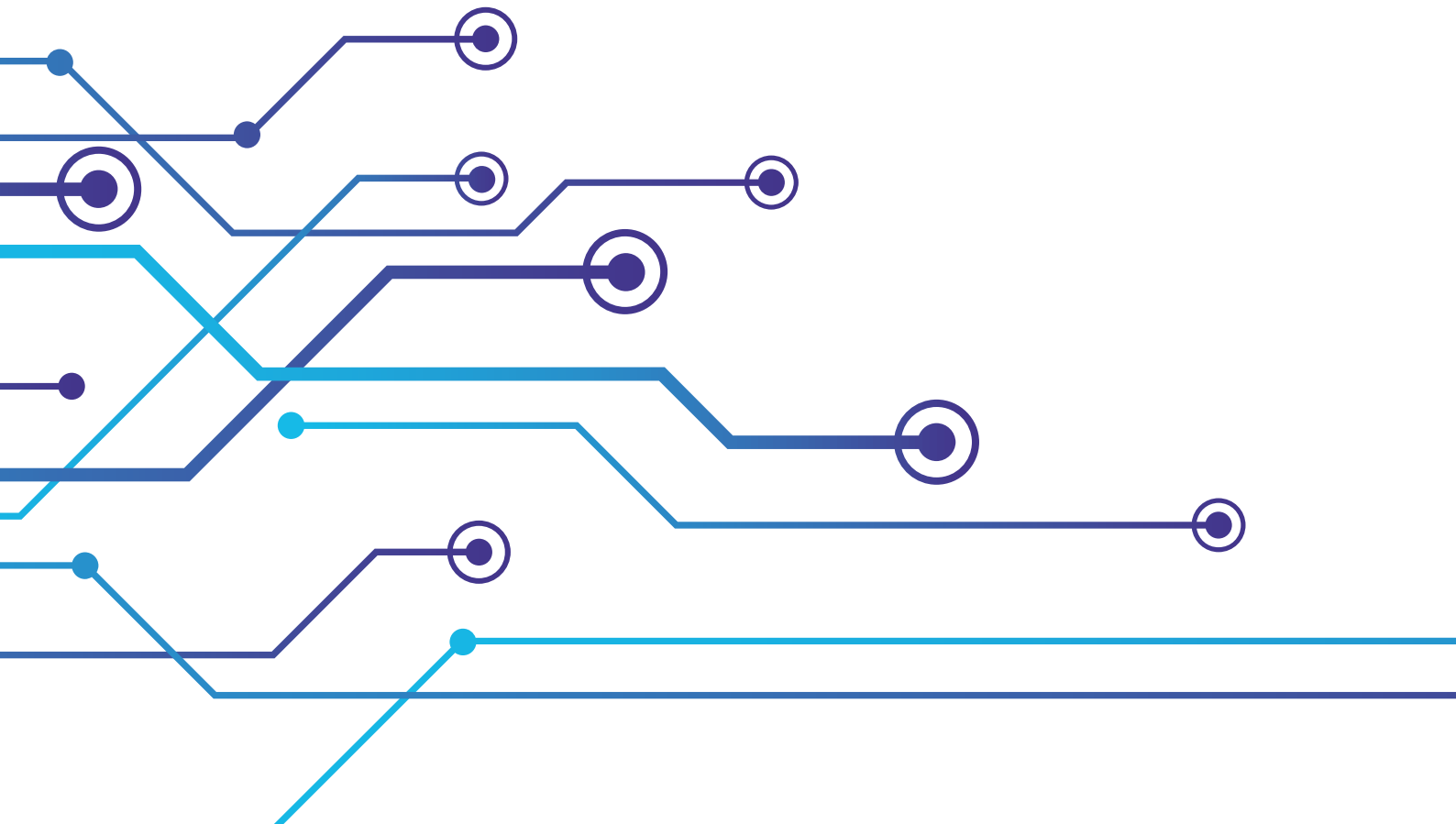
•
Age of Universe

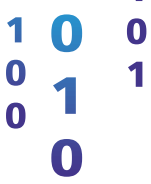
Time required to break AES-128

How long does it take to break AES-128 with today's technology?



- RSA key size recommendations
- development of quantum computes
- successes in breaking RSA



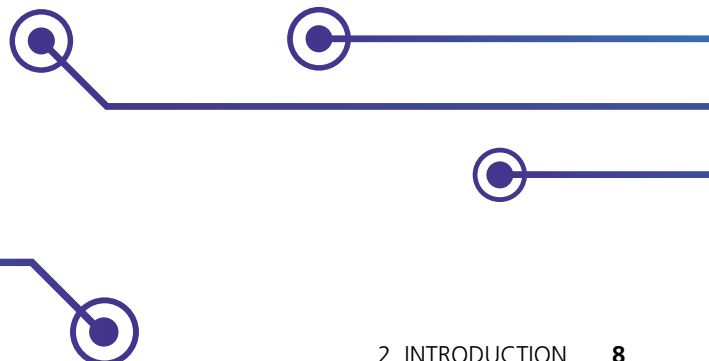


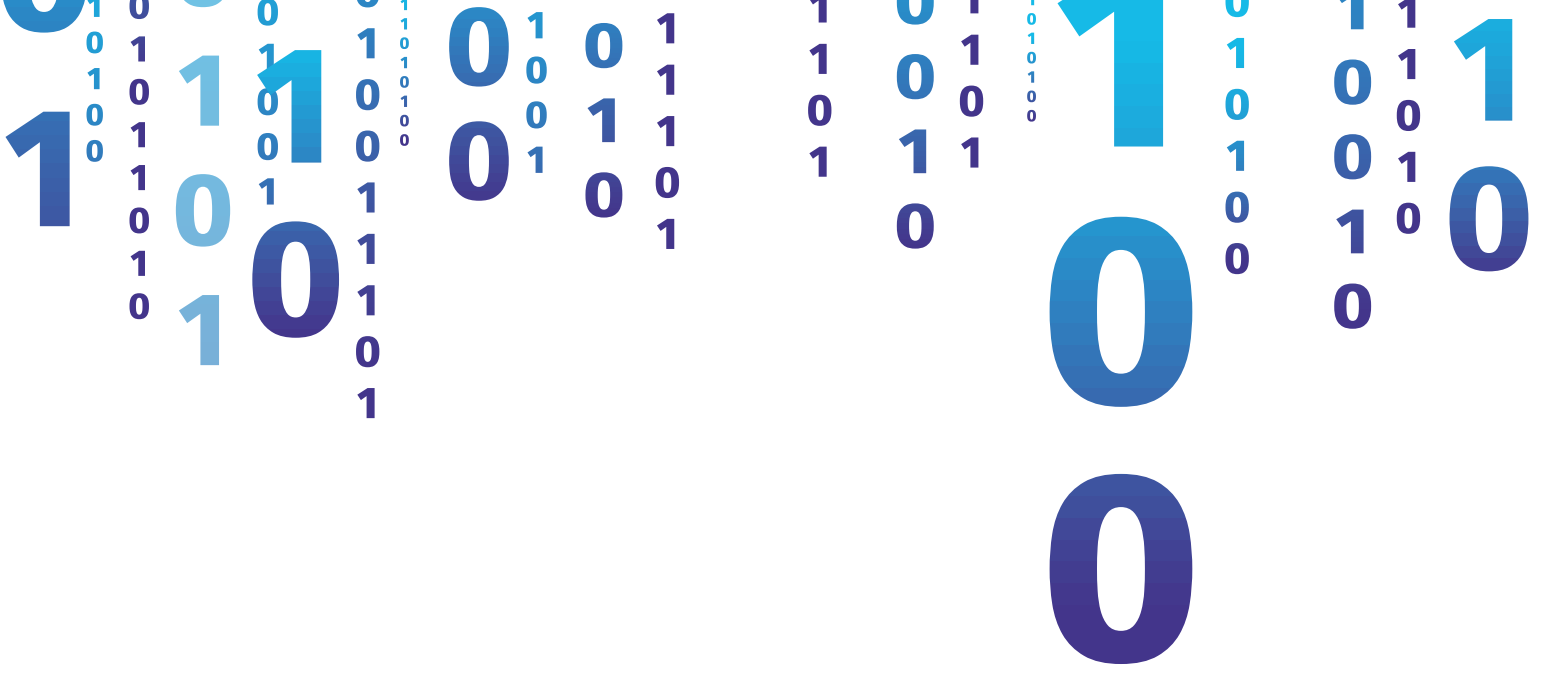
Another example is the hash standard Message Digest 5 (MD5) that was developed by Ron Rivest in the early 1990s. In 1995, NIST standardized a variant of MD5 as SHA-1. A short time after Ron Rivest published MD5, researchers found weaknesses in MD5. In 2004 academics successfully performed collision attacks on MD5. In 2008 researchers produced a rogue certificate (it was indistinguishable from the valid certificates of the certificate authority) based on MD5 hashes that enabled them to create certificates for arbitrary internet domains and therefore impersonate any website, e.g., Google, Facebook, banks, governmental websites, and mail providers. In 2002, NIST standardized SHA-2 as a secure alternative to MD5 and SHA-1 and, in 2015, SHA-3 after an eight-year long public standardization process. Nevertheless, MD5 is still in use today.

Such examples show that in worst case scenarios entire cryptographic primitives may need to be replaced due to significant progress in cryptanalysis or computational power. In other cases, it might be sufficient to increase security parameters of primitives like the length of a cryptographic key. When the asymmetric encryption scheme RSA was introduced in the 1970s, it was commonly accepted to use 512-bit or 768-bit keys. In the 1990s, RSA Laboratories opened the RSA Factoring Challenge. RSA Laboratories published a series of RSA keys of different key sizes and the goal of the challenge was to provide factorizations of these keys. Very quickly, several challenges were broken and RSA Laboratories recommended to use 768-bit to 1024-bit RSA keys. In 1999, RSA-512 was for the first time publically broken and in 2002 NIST recommended to use 1024-bit keys. In 2010, researchers were able to break RSA-768 after performing a two-year long computation. In 2011, NIST recommended to use 2048-bit keys and in 2016 NSA recommended to use 3072-bit keys. Therefore, in the last 20 years, there have been three changes in the recommended key length for RSA keys.

Sometimes cryptographic standards or implementations are based on wrong assumptions. For example, cryptographers believed that there was no harm in using the same prime modulus for all implementations of the Diffie-Hellman key exchange. Today we know that this allows an attacker to break an arbitrary number of connections easily once he manages to break this shared modulus. If a different modulus is used for each key exchange, breaking one million connections is one million times more expensive than breaking one single connection. If the same modulus is used for one million connections, breaking one million connections is just slightly more expensive than breaking one single connection, which makes it very valuable for an attacker even if he has to spend a high cost for breaking the modulus. This was exploited (among other weaknesses) in the (academic) Logjam Attack in 2015.

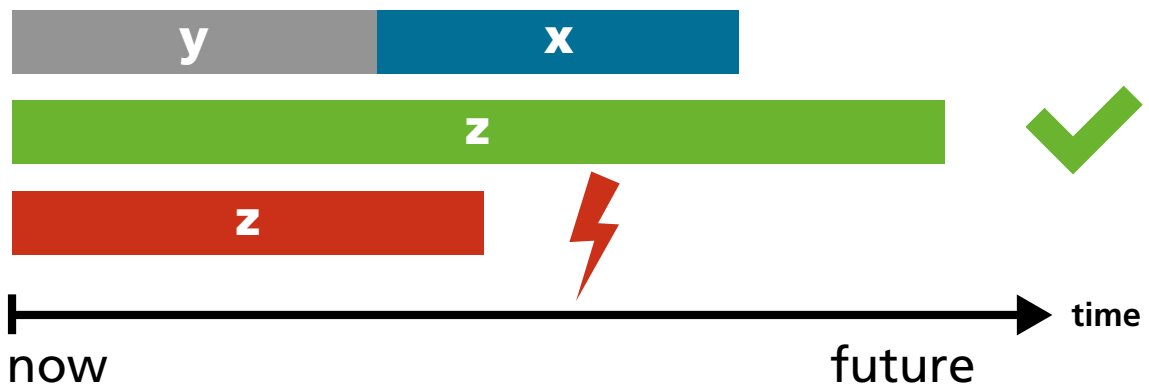
All these examples show that cryptographic primitives, parameters, and principles erode over time. Every once in a while, the key length needs to be extended; occasionally, entire cryptographic primitives need to be replaced by new and secure alternatives. Therefore, processes and products that are relying on cryptography must be maintained and potentially updated during their entire lifetime. The earlier this requirement is incorporated into the design process of a secure system, the cheaper the transition to new parameters and primitives becomes.





Open question: How big is the threat by quantum computers?

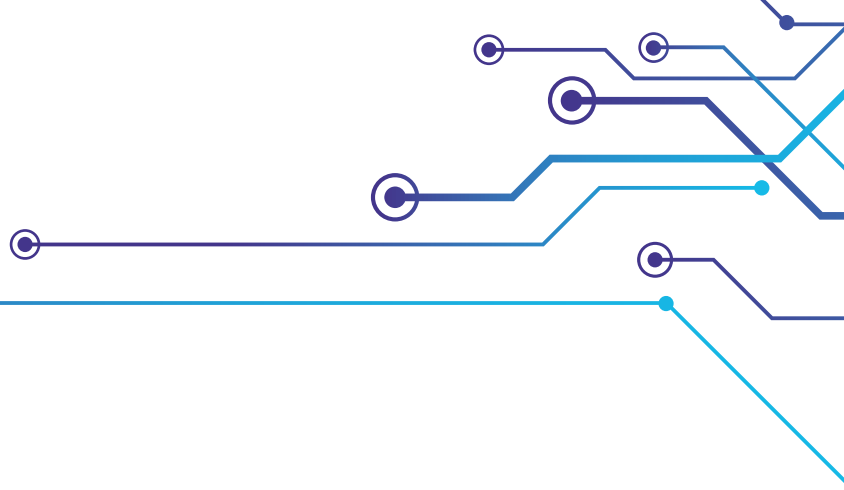
Since it is hard to predict z, the question remains open.



x: time that secrets must remain secret
y: time it takes to deploy quantum-computer secure cryptography
z: time it takes until quantum computers break current cryptography

If z is larger than x+y, we are fine. If it is smaller, we are in danger!

1 0 0
0 1 1
0 0 1



2.2 POST-QUANTUM CRYPTOGRAPHY

Quantum computers pose a severe threat on today's cryptography: If sufficiently large quantum computers can be built, they will be able to break asymmetric cryptography, e.g., RSA, ECC, DH, DSA, and ECDS in practical time using Shor's quantum-algorithm. Asymmetric cryptography is used for authentication, key exchange, digital signatures, and certificates in the Internet and in secure applications. In addition, symmetric ciphers like AES will be under threat by quantum computers using Grover's quantum-algorithm. Symmetric ciphers are used to encrypt data in transit (e.g., in the Internet) or at rest (e.g., hard-drive encryption). Experts recommend doubling the key size from 128 bit (AES-128) to 256 bit (AES-256) in order to defend against large, powerful quantum computers. Therefore, all cryptography that is used in the Internet today and in many other sensitive applications are under threat by quantum computers.

Cryptographers are working on alternative encryption schemes in particular for asymmetric cryptography that are not known to be affected by quantum computers. This field of cryptography is called "post-quantum cryptography". There is a broad range of hard mathematical problems where quantum computers are not known to provide a groundbreaking advantage, e.g., problems in coding theory, lattice theory, solving multivariate polynomials, and isogenies on elliptic curves. Furthermore, secure hash functions can be used to construct signature schemes. There is an ongoing debate on which approach gives the most secure and efficient crypto systems. NIST started a standardization process for post-quantum cryptography in 2017. Therefore, there should soon be practical schemes available that are robust against attacks using quantum computers.

A common disadvantage of most of today's post-quantum schemes is the higher demand for resources compared to classical cryptographic schemes. Usually the key sizes of private and public keys are larger, the encoded cipher text and signatures are longer, and the computational demands tend to be higher. This is in particular troublesome for embedded systems with low resources as well as Internet servers that have to handle a large number of secure connections. There is ongoing academic research on reducing the resource requirements of post-quantum schemes while maintaining their security. Furthermore, some schemes have additional requirements compared to classical schemes that are currently in use. For example, some hash-based signature schemes need to store a state that is altered after each signature. Returning to a previous state breaks the security of the signature scheme. This poses new requirements on the backup strategy for secret signing keys.

A typical requirement for secret or sensitive data is that it must be kept secure for at least x years, where x depends on the sensitivity of the data. If we require y years for the transition to post-quantum cryptography and assume that large quantum computers arrive in z years, then $y + x$ must be smaller than z . Otherwise, secrets that are transmitted at the end of the pre-quantum era can be stored and consecutively be broken once quantum computers become available before these secrets lose their sensitivity. If we wait with the transition to post-quantum schemes until we are sure that quantum computers pose a practical threat it might already be too late for protecting our secrets. Also, one has to keep in mind that quantum computers are only one of many cryptographic threats. So, even if quantum computers that may be able to break current cryptography may never be built, we need to provide sufficient flexibility to respond to possible future threats due to developments in classical cryptanalysis and classical computing power.



For further reading:

Practical Post-Quantum Cryptography

R. Niederhagen, M. Waidner, 2017

Fraunhofer SIT

www.sit.fraunhofer.de/de/reports/#c4742

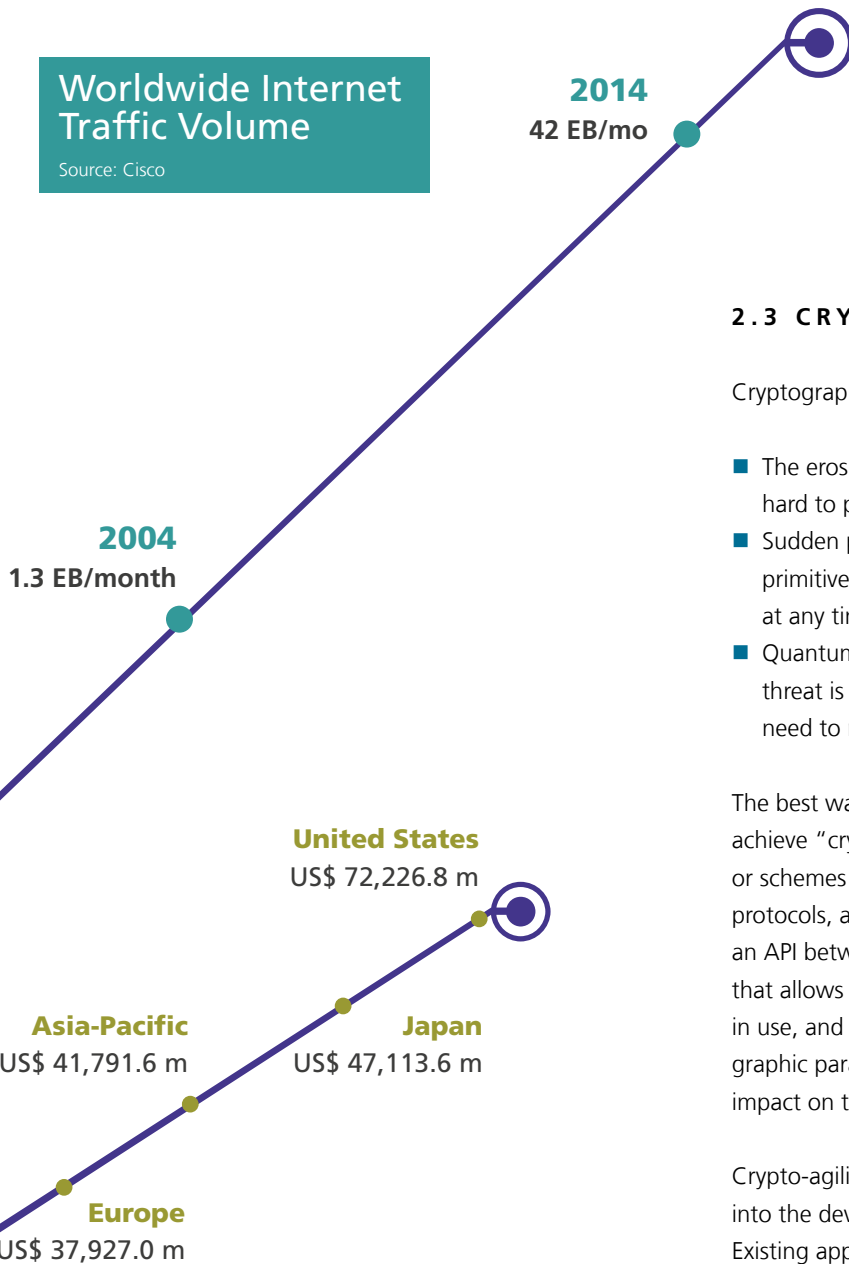


1994
29 TB/month

1984
15 GB/month

Worldwide Internet Traffic Volume

Source: Cisco



Global Market Outlook for the Hardware Encryption Market in 2020

Source: Global Industry Analysts

2.3 CRYPTO-AGILITY

Cryptography is a very dynamic technology:

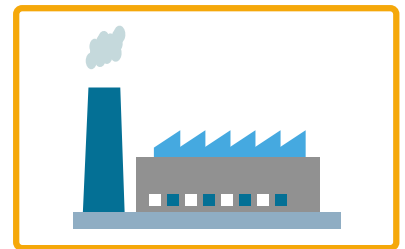
- The erosion of cryptographic parameters and primitives is hard to predict.
- Sudden progress in cryptanalysis may force us to replace primitives, to fix implementations, or to increase key sizes at any time.
- Quantum computers will not arrive overnight but their threat is severe enough that we should prepare for the need to make a transition to post-quantum schemes.

The best way to prepare for these dynamic changes is to achieve “crypto-agility”, i.e., the ability to change parameters or schemes dynamically while maintaining the operation of protocols, applications, and processes. Crypto-agility requires an API between a crypto-layer and the rest of an application that allows to hide the details of the cryptographic primitives in use, and therefore enables the replacement of cryptographic parameters or primitives without (or with only small) impact on the rest of the application.

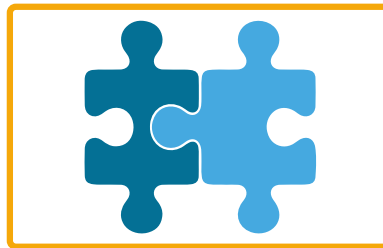
Crypto-agility should be incorporated from the very beginning into the development of secure processes and applications. Existing applications should be upgraded to enable crypto-agility. If an application is scheduled to be updated, e.g., from RSA to elliptic curve cryptography (ECC), this upgrade should not replace a fixed RSA implementation by a fixed ECC implementation, but it should enable to replace the new ECC primitives with future primitives easily and dynamically, when needed. This requires research in standardizing cryptographic interfaces for typical use-cases and applications so that the underlying primitive can be exchanged with minimal impact on the rest of the system.



CONSUMER



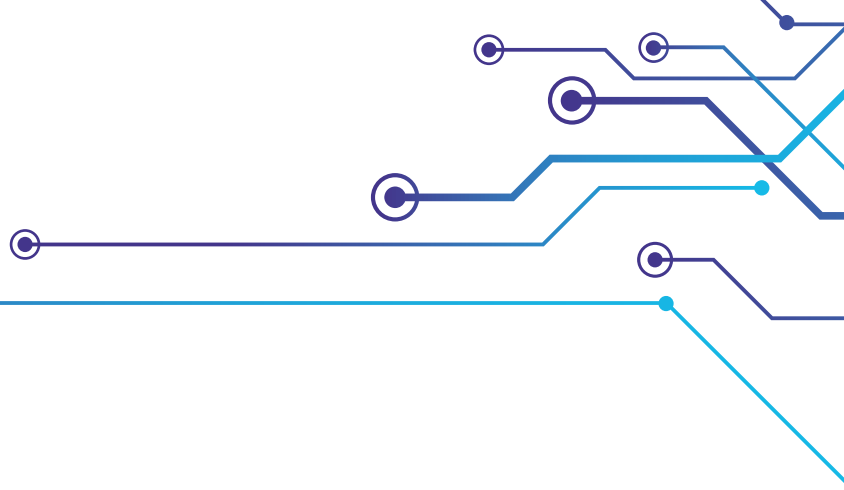
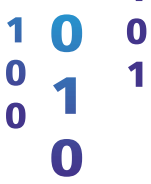
OEM



CRYPTO
SUPPLIERS



3. CRYPTO-READINESS OF THE INDUSTRY



Cryptography is one of the main technologies that are used to achieve IT security today. Since digital communication is the main pillar of our modern society and economy, cryptography plays an important role in virtually every economic sector. There are three major groups of industry categorized by how they interact with cryptography:

1. Most companies implicitly use IT solutions that incorporate cryptography in order to achieve security. Companies that plainly consume cryptography do not care about the technical details. They are using off-the-shelf products that are provided by OEMs.
2. OEMs often do not implement cryptography themselves, but integrate external cryptographic libraries or modules into their products. OEMs do not need to understand the details of the cryptographic implementation, but they must know which cryptographic primitives and parameters are required for their products.
3. Crypto suppliers provide the actual implementations of cryptography to OEMs in the form of cryptographic libraries and modules.

All these players are facing individual challenges.


3.1 CHALLENGES FOR INDUSTRIAL CONSUMERS OF CRYPTOGRAPHY

Examples for industrial consumers of cryptography are companies that require secure IT products for their everyday processes, e.g., secure storage of data on mobile devices, secure virtual private network solutions, and private communication. These companies require off-the-shelf, ready-to-go solutions and have no interest in the technological details that the vendors implemented to provide security. They want to make sure their investments pay off, but they cannot invest resources to assess and compare products from different vendors in order to choose a specific solution.

These industrial customers want to have an easy mapping from their use-cases to the best and cheapest product without the need to understand neither the precise security requirements of the use-case nor how the vendor technically fulfills these requirements. Industrial consumers of cryptography would like to have an official catalog that maps use-cases to product classes and an independent certification that a given product fulfills the security requirements defined for these use-cases.

Key Size and Message Size

CLASSICAL SCHEMES

 
RSA-2048

 
RSA-4096

 
ECC
256-bit

 
ECC
512-bit


DH
key exchange


ECDH
key exchange



KEY EXCHANGE




New Hope
lattice based


SIDH
supersingular
isogenies

PUBLIC-KEY SIGNATURES

 
XMSS
(stateful)
hash based

 
SPHINCS
(state free)
hash based

 
HFEv
multivariant based


PUBLIC-KEY ENCRYPTION

 
McEliece
code based

 
Kyber (KEM)
lattice based

Post-Quantum Cryptography

 = size of the corresponding public key.

 = data length, e.g., the key-exchange message length or the length of the cipher text.

Probability that some fundamental public-key crypto will be broken by quantum.

Source: Dr. Michele Mosca

one-in-seven

one-in-two

today

2026

2031



3.2 CHALLENGES FOR INDUSTRIAL INTEGRATORS OF CRYPTOGRAPHY

OEMs require high-quality implementations in regard to performance, efficiency, and security. Open source libraries provide publicly reviewed and easy-to-use cryptography. However, OEMs require long-term support and quick incidence response, which is often not guaranteed by Open source projects: Security patches need to be provided for a long period of time; special requirements of the OEM's customers need to be incorporated quickly.

OEMs need to make decisions on the security design based on their customers' requirements, and need to request the correct primitives and implementations from their crypto suppliers. These decisions have a far-reaching impact on the security and performance of the product. Often, there is a very broad field of cryptographic primitives to choose from, each one with its specific requirements and features. An example is the field of elliptic curve cryptography (ECC). For ECC, the designer needs to choose a specific curve as basis for the cryptographic primitives. Despite the fact that there is a broad consensus on the security requirements for the curve selection, there is a huge number of different curves promoted by different standards, companies, and security experts.

In the USA, curves standardized by NIST are commonly used. However, recently these NIST-curves have received some scrutiny due to suspected involvement of the NSA in the choice of the curves. Furthermore, these curves are not necessarily the best choice in regard to performance and efficiency. In Germany, the German Federal Office for Information Security (BSI) recommends to use the so-called "brainpool" curves. Also, these curves are criticized to have been defined without taking performance and efficiency into consideration. Another option is the highly efficient and optimized curve "curve25519" designed by the cryptographer Daniel J. Bernstein, explicitly targeting performance as design criteria. However, this curve is currently in the standardization process by the IETF for the upcoming TLS 1.3 standard, but is not otherwise standardized. Choosing from this broad range of curves is a challenge for OEMs.

3.3 CHALLENGES FOR INDUSTRIAL CRYPTO-PROVIDERS

Crypto suppliers actually implement cryptographic primitives and protocols and provide cryptographic libraries and solutions to OEMs. In many cases they are using libraries from Open source projects. Crypto suppliers often do not know for what specific applications and products their libraries are going to be used. Therefore, they need to provide a broad range of parameters and primitives but are not always able to optimize for specific use cases or platforms. In order to be competitive, they need to be cheap which again prevents them to optimize their implementations and to fit them to the OEM's actual environment and use-case. Crypto suppliers are restricted to provide standardized cryptography. Their customers do not usually request new, not yet standardized solutions. There is no market for 'orchids'; solutions must be cheap, standardized, off-the-shelf, and easy to use.



4. PROBLEMS TO GET WORSE IN THE FUTURE

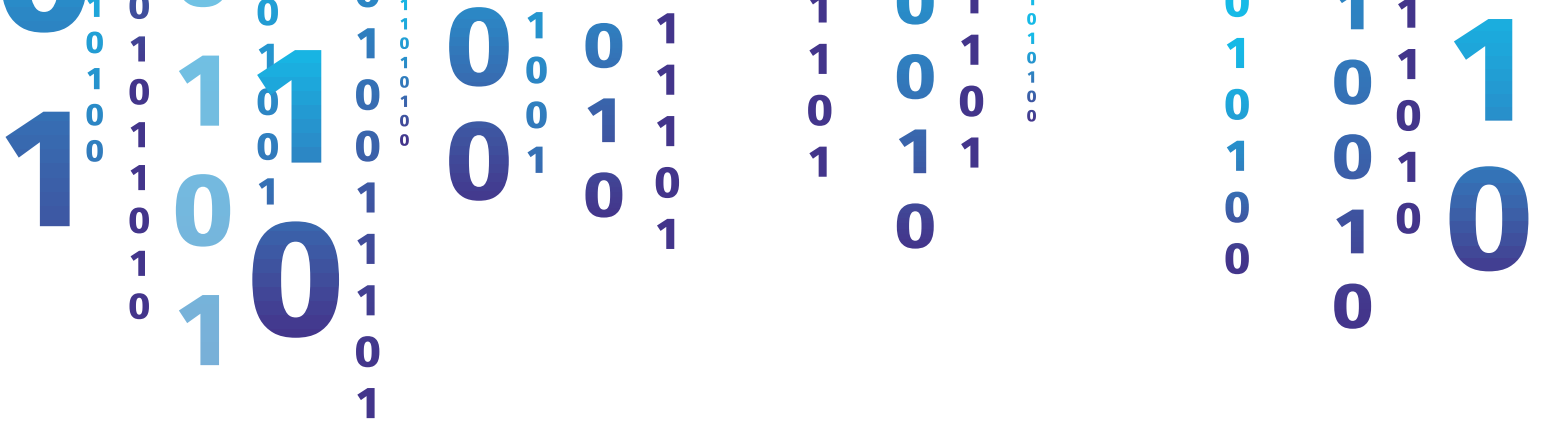
1 0 0
0 1 1
0 0 0

Today's applications are not sufficiently flexible in regard to cryptography. In large systems that have been growing over time with contributions from several teams, the same cryptographic primitive often is implemented independently several times. For example, a desktop client, a mobile client, and the corresponding server each might have (several) individual SHA-1 implementations, because their components were implemented by different teams. If now SHA-1 needs to be replaced by a more secure alternative (e.g., SHA-2 or SHA-3), all individual implementations of SHA-1 need to be identified and replaced. This makes crypto-agility very expensive or even prevents it. If all clients and the server used the same crypto library, it would be much easier to provide consistently updated versions of all applications.


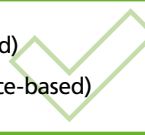
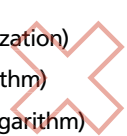






Therefore, it is necessary to make crypto-agility part of the system design from the very beginning. Every newly started system development that requires cryptography must take crypto-agility into account. This includes a secure update strategy, a primitive-agnostic crypto API, and agile cryptographic protocols.

If crypto-agility has not been part of the design for a given system, the system must be adapted as soon as possible to achieve crypto-agility. This can be performed incrementally as long as the cryptographic parameters and primitives in use are still secure. With each scheduled update more and more cryptographic modules should be re-written in order to use a crypto API; individual implementations of cryptographic primitives should be replaced by calls to a crypto library. Additionally, attack vectors like downgrading schemes, attacks during cipher negotiation, etc. have to be considered. During this transition time, protocols should be modified to allow different parameters and primitives in a backwards-compatible manner. Once all system entities have been migrated and crypto-agility has been enabled over the complete system, outdated protocols, primitives, and parameters should be disabled.

In the worst case, cryptographic primitives or parameters become insecure for a complex system that does not support crypto-agility at all or that is in transition to become agile. In this case, the system remains vulnerable until all components have been fixed. The cost to achieve a secure system increases due to the high pressure and the small timeframe. If attackers are able to exploit cryptographic weaknesses during this time, secrets may be irreversibly exposed.

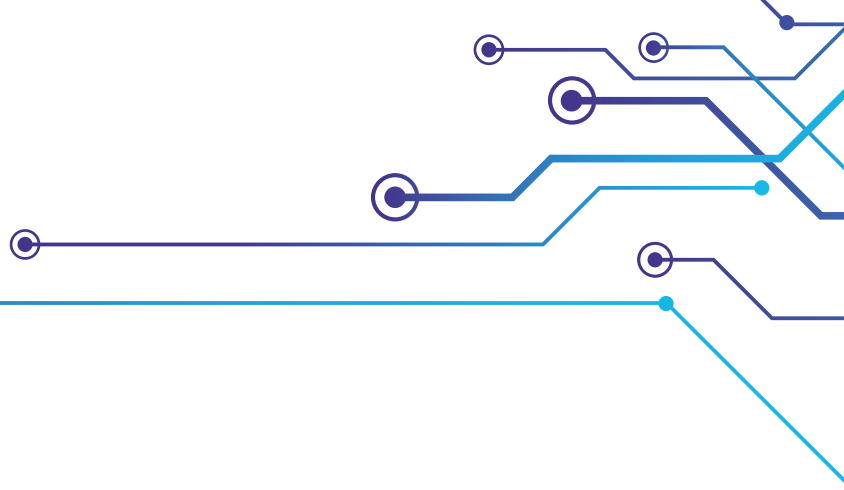


What schemes are broken by Post-Quantum Cryptography?

	CLASSICAL	POST-QUANTUM
PUBLIC KEY ENCRYPTION	RSA (integer factorization) ECC (discrete logarithm) 	McEliece (code-based) Kyber (KEM) (lattice-based) 
SIGNATURES	RSA (integer factorization) DSA (discrete logarithm) ECDSA (discrete logarithm) 	XMSS (hash-based) HVEv- (multivariate) 
KEY EXCHANGE	DH (discrete logarithm) ECDH (discrete logarithm) 	NewHope (lattice-based) 
SYMMETRIC KEY ENCRYPTION	AES-128 	
	AES-256 	
HASH FUNCTIONS	SHA2 SHA3 	

5. SEVEN RECOMMENDATIONS FOR NEXT GENERATION CRYPTOGRAPHY

1 0 0
0 1 1
0 0 1



In the following sections, we make seven recommendations on how to transition to the next generation of cryptography in order to achieve better and more secure IT systems.

5.1 PUBLIC AWARENESS AND UNDERSTANDING OF CRYPTOGRAPHY

Since digital communication is ubiquitous in our modern society and a backbone of our economy, the public, politicians, and decision makers in industry need to understand the very basics about cryptography, not necessarily on a technical level but concerning what it can provide and what it cannot.

Recommendation: For a short-term impact, policy makers should establish a certification program that gives an incentive to decision makers (in industry and politics) to attend basic training programs on IT security and cryptography. For a middle- and long-term impact, policy makers should add lessons on IT security and cryptography to the school curriculum at junior high and high school level (in an age-appropriate depth) in all member states.

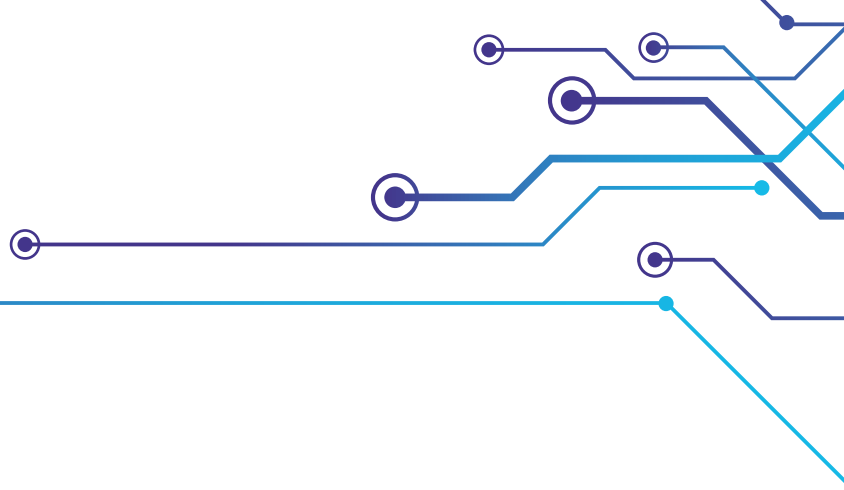
Benefit: Early education and vocational training on the basics of IT security and cryptography will raise public awareness of IT security in the long-term and enable individuals to make better decisions on how to protect information, privacy, and intellectual property in the age of the Internet. Training programs for decision makers will improve policies and processes on IT security.

To policy makers on EU, federal, and state levels
(esp. ministries of education, governmental or official
institutions for vocational training)





1 0 0
0 1 1
0 0



5.2 EU-STANDARDS FOR CRYPTOGRAPHY

Companies require strong EU-wide standards for cryptography.

Recommendation: The EU should strengthen the role of an existing EU-supranational agency (for instance ENISA) or initiate a new standardization agency in order to provide EU-wide standards for IT security and cryptography. Cryptographic standards passed by this agency must be accompanied by reference implementations and test cases in order to support implementers and to help avoiding bugs.

Benefits: This gives customers trust in critical systems and enables companies to sell or purchase cryptographic systems easily within the EU. Such standards will also influence non-EU standardization, e.g., in the US, Asia, and for Internet protocols. This increases the influence of European players all around the world and facilitates system development for a large market.

To policy makers on EU level, and to industry.

5.3 FUNDING OF APPLIED AND INTER-DISCIPLINARY CRYPTOGRAPHIC RESEARCH

To achieve crypto agility on a big scale it needs research on applied IT security and cryptography. Large, interdisciplinary research teams should develop practical solutions that can be incorporated into products and systems within the next one to five years. The goal is explicitly not basic research but the application of well-established academic solutions in industry and consumer products.

Recommendation: All stakeholders should provide additional research funding specifically for interdisciplinary applied research in IT security and cryptography. The new National Research Center for Applied Cybersecurity (CRISP in Darmstadt) should be strengthened to become the spearhead center of Europe.

Benefit: Applied and interdisciplinary cryptographic research helps industry to develop and integrate top-notch practical crypto-solutions that can be incorporated into products and systems.

To all stakeholders.



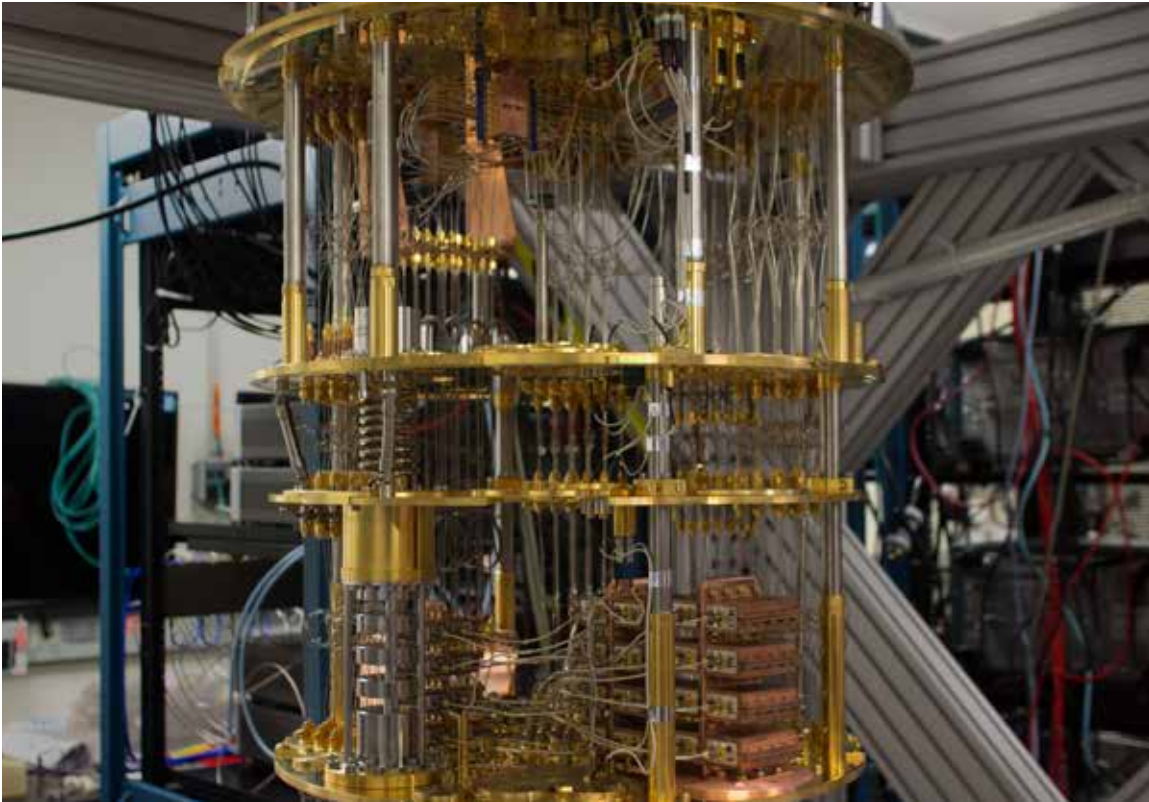
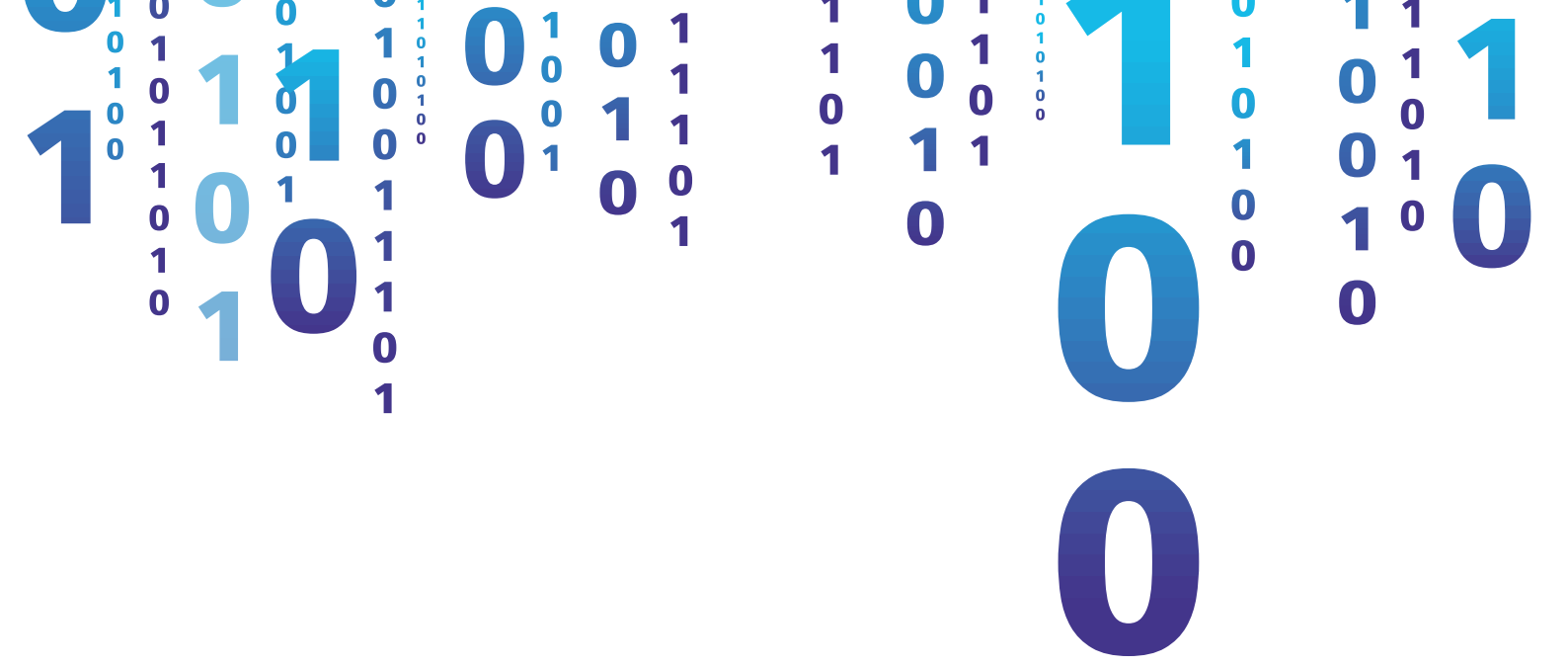
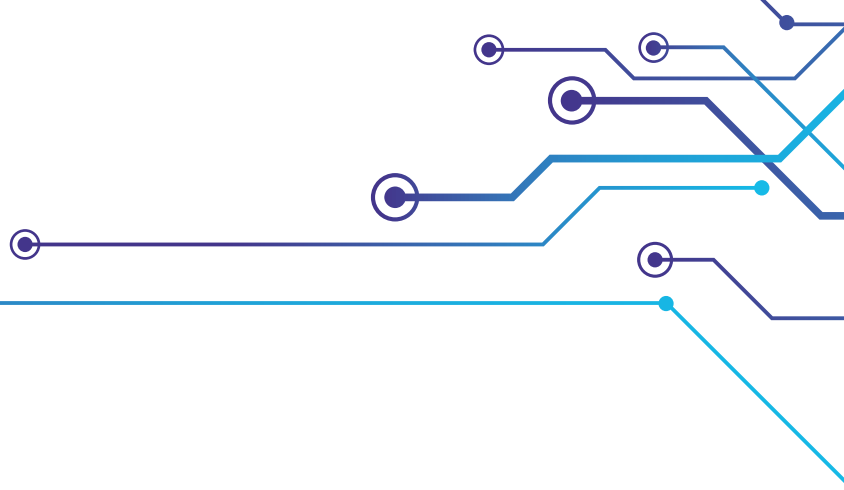


Photo of IBM quantum computer.

(Credit: IBM Research)



5.4 COUNCIL OF CRYPTO SAGES

Political decision-making, standardization, and long-term planning of budgets for academic and basic research of upcoming future technologies need the support of experts. Neither politicians nor standardizations officers can keep track of advances and challenges in IT security and cryptography. They require the counselling of distinguished experts in the field.

Recommendation: The EU should establish a “Council of Crypto Sages” that has the expertise to recommend cryptographic primitives, parameters, and protocols and that is able to consult governments, the EU, and standardization agencies in technological questions about cryptography and IT security. Besides providing expertise on solutions that can be incorporated today or in the near future, these Crypto Sages also look far into the future and determine promising technologies that might lead to game changing innovations.

Benefit: The creation of a council of crypto sages enables solid and informed decision-making and long term planning of research programs.

To policy makers on EU level.

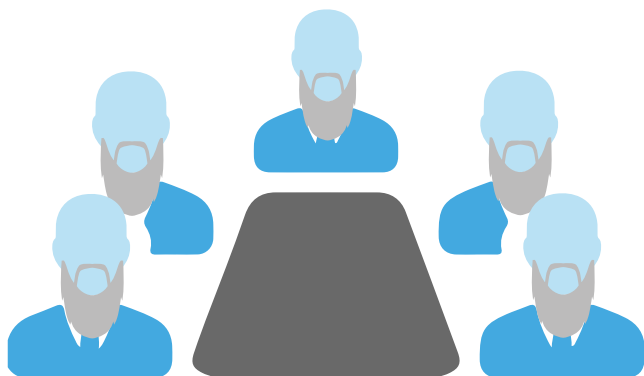
5.5 COOKBOOK FOR CRYPTOGRAPHIC SOLUTIONS

Modern IT systems face plenty of security requirements, attack scenarios, and privacy regulations. For system developers, it is hard if not impossible to select the correct cryptographic solution from the vast set of possible approaches.

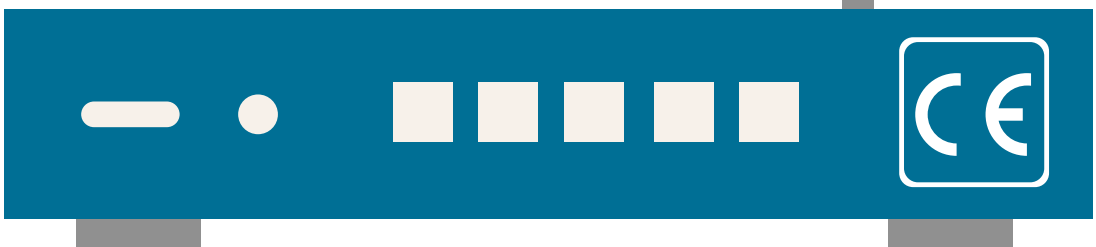
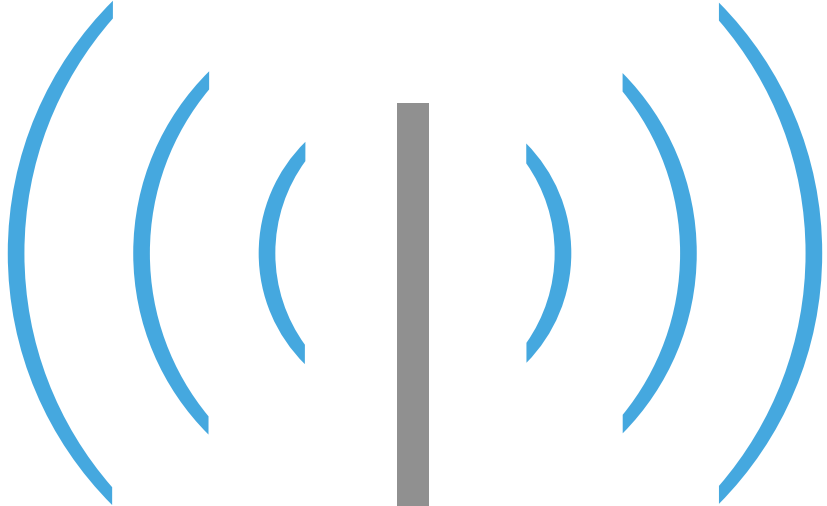
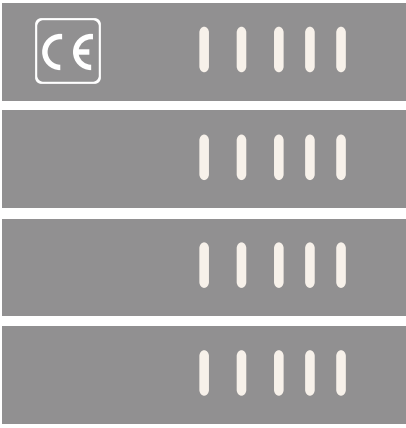
Recommendation: Industry and policy makers should provide funding for an institution that provides and maintains a crypto cookbook. This institution gets the task to design the cookbook based on feedback from industry, academia, and governmental agencies in order to cover uses-cases that are relevant for industry and to provide state-of-the art solutions. The institution updates the crypto cookbook annually. Each update is presented at a dedicated event in order to achieve high media coverage and public awareness.

Benefit: The up-to-date cookbook supports industry in producing secure and efficient cryptographic solutions at lower cost.

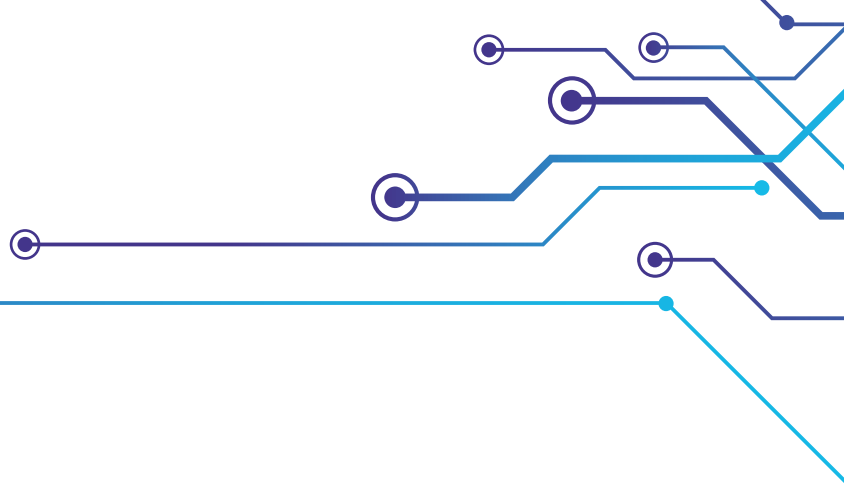
To industry, policy makers on EU, federal, and state levels, and institutions of applied research.



01010110110
10011011010
00011011010
10101101101
00101011011
01001101101
10001101101
00101011011
10001101101
00101011011
10001101101
11101101101
11011011011
00101011011
00101011011
01010110110
11010110110
11010110110
11010110110



1 0 0
0 0 1
0 1 0



5.6 MINIMAL REQUIREMENTS FOR CRYPTOGRAPHIC SOLUTIONS

Similar to vaccination improving the security of the entire population, increased security of many IT systems will improve the security of the entire Internet. However, increasing the security of IT systems is expensive. Often, companies choose a cheaper but less secure solution.

Recommendation: Policy makers should (with the Crypto Sages' support) define and enforce minimal security standards for IT systems. For this purpose, the CE marking should be extended to IT security or a similarly dedicated label should be established. Products that do not fulfill these minimal requirements are not to be allowed on the EU market. These minimal requirements should eventually also cover crypto-agility and lifetime security updates.

Benefit: Minimal requirements for cryptographic solutions improve the security of business and the public.

To policy makers on EU level (supported by applied research institutions) and to industry.



5.7 INVENTORY ANALYSIS OF CRYPTOGRAPHIC FUNCTIONS

When a cryptographic primitive is suddenly broken or a critical bug in a security library is found, companies have to figure out quickly if and where this primitive or library is used in their products or processes. Starting to search in the source code or system once an incident has occurred costs time and resources, and increases the time span of exposure and thus the risk of a successful attack.

Recommendation: Ideally, all companies that use or provide IT systems should set up and maintain an inventory of all cryptographic primitives and security libraries they use. However, such a regulatory requirement would pose too much of a burden on industry. In order to achieve this kind of industry-wide IT-security inventories, we recommend three phases: First, governments and the EU should establish such an inventory for their own systems and processes, and contractually require companies that provide and maintain the systems to deliver the required information. In a second step, companies that offer IT products should be required to offer a list of all cryptographic primitives and libraries used in their product. Finally, all companies that use IT systems should be required to maintain the inventory. The entire process should span over several years in order to allow industry to adapt to these requirements. The inventory must be kept up-to-date for each software release and on a regular (e.g., half-yearly) basis.

Benefit: The response time from a security incident to a system-wide fix will be reduced significantly. This allows companies to react more quickly to security threats, thereby saving money and protecting business secrets. The entire society will benefit by having more secure applications and a safer Internet.

To industry.

Most Common Countries for Encryption Products:

Source: Schneier (February 2016)

Number of products:



304



112



54



47

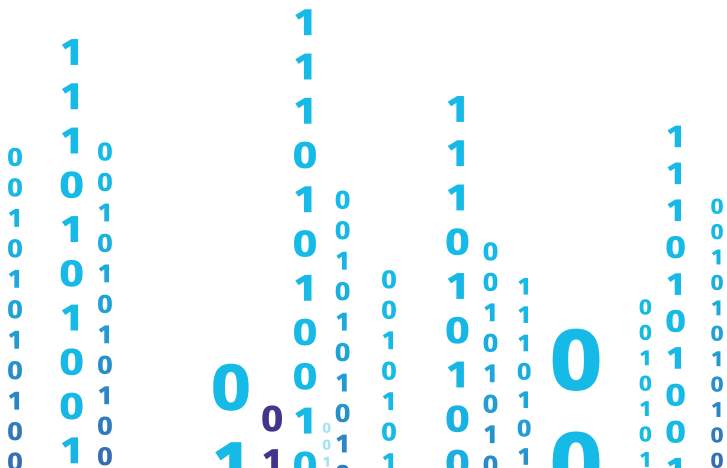


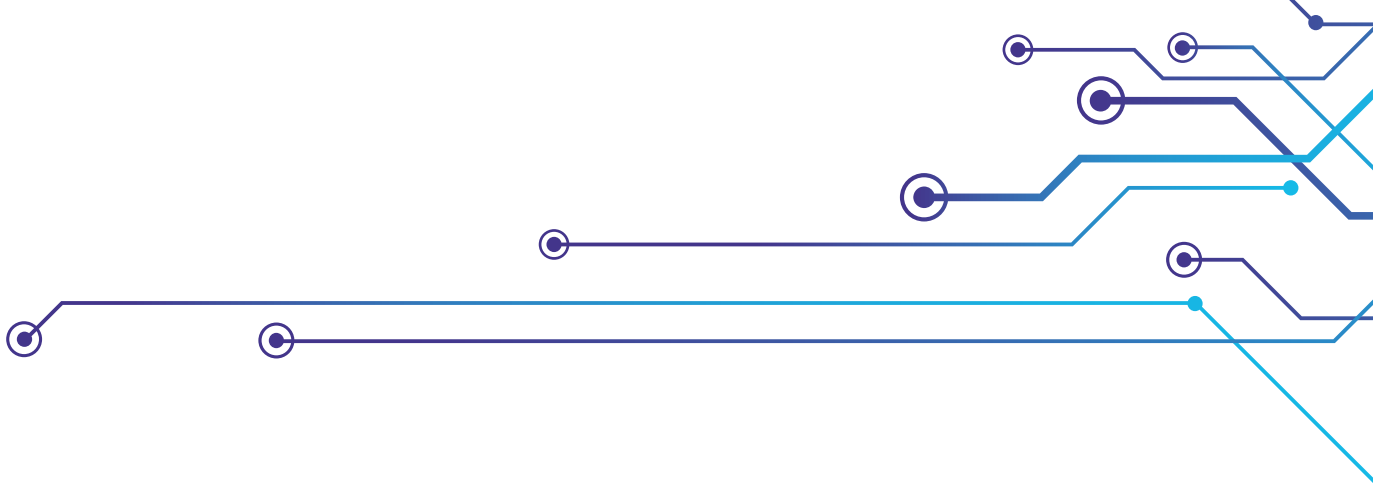
41



33

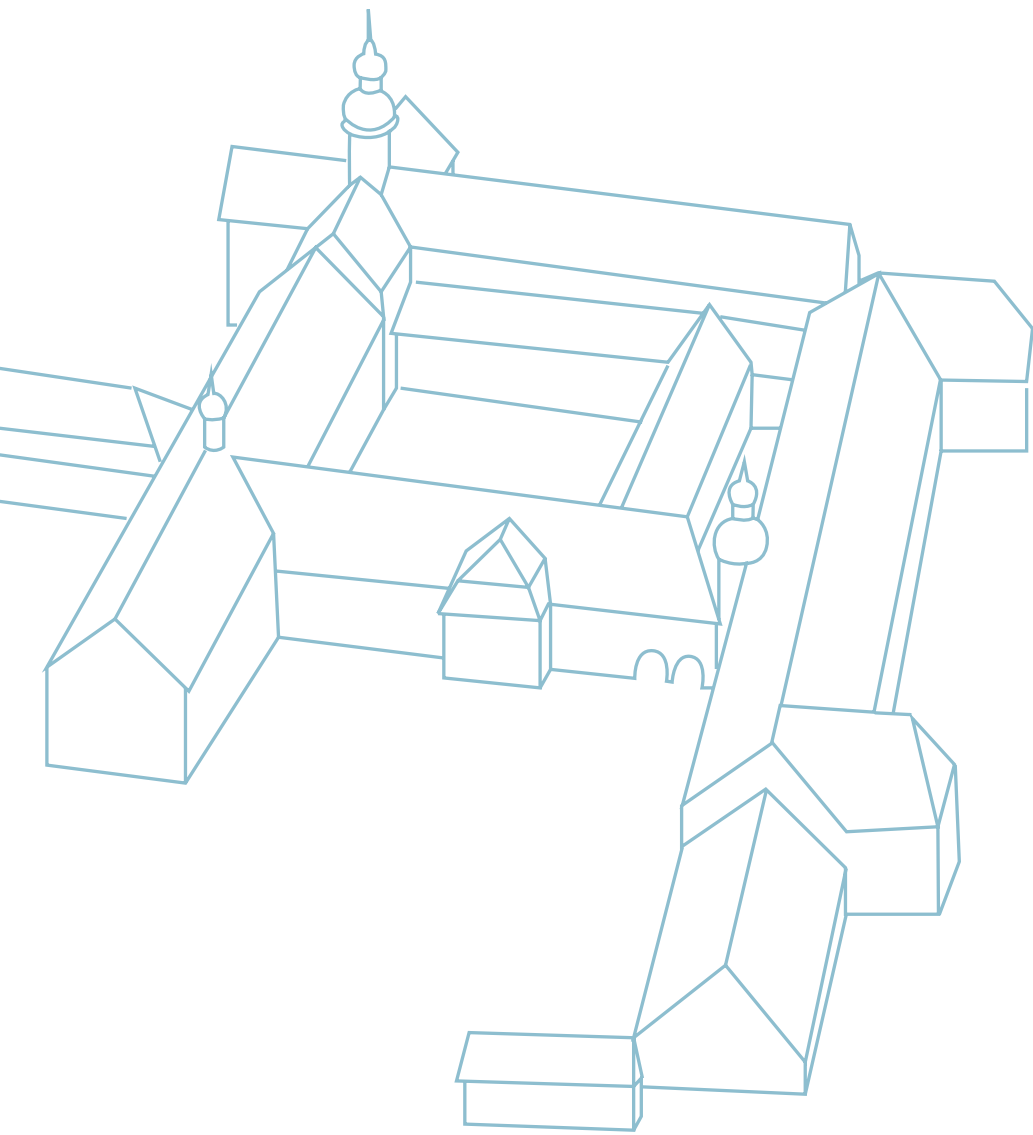
CONCLUSION

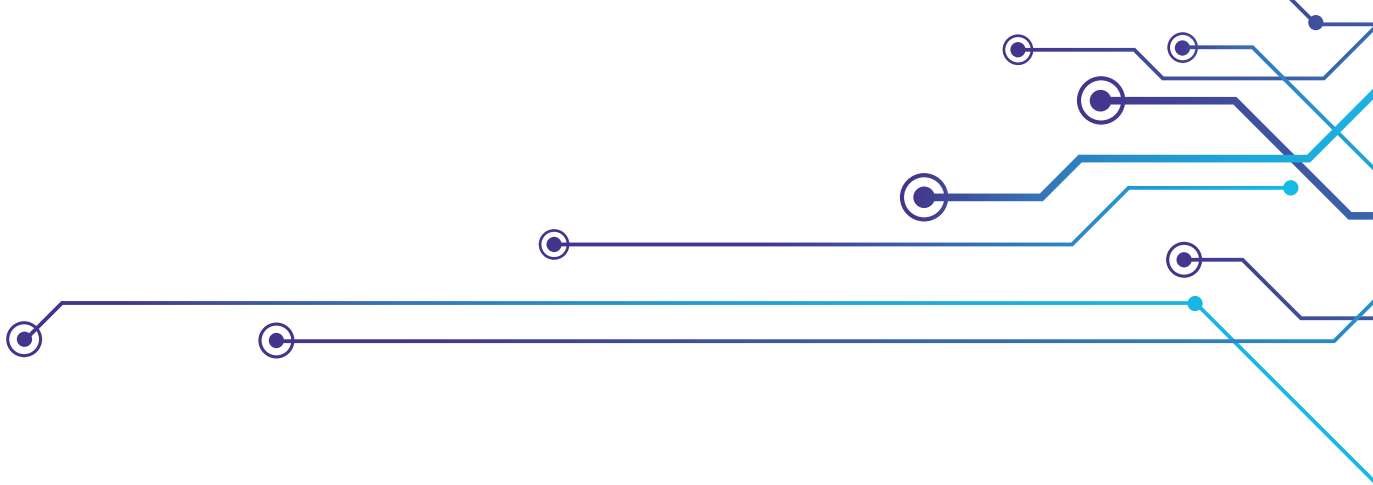




Though there are many security challenges to be faced every day, the risks to cryptographic security posed by technological advancement and quantum computing in particular are of a different order. A vulnerability that affects one product or service is restricted in its impact whereas the breaking of a cryptographic primitive may render a multitude of applications insecure and has the potential to shake the fundamental trust people have in wide parts of the Internet and its functionalities. Even significant vulnerabilities, like the ones exploited by the Spectre and Meltdown attacks on CPU, that affect a vast amount of different IT systems can be fixed with a software update or hardware upgrade. However, if a cryptographic algorithm is broken, all transmitted data that was encrypted with this algorithm will immediately and irreversibly be revealed and become insecure. Therefore quantum computers and other developments with similar cryptographic impact may cause damage to wide parts of our economy and even endanger whole societies. The transition to crypto-agility and next generation cryptography needs much time and preparation and can only succeed if there are cryptographic alternatives available.

European decision makers from industry and the public sector need to become aware of this and make crypto agility a strategic priority. China and other countries are investing heavily in research in quantum computing, making it just a question of time until cryptography will change forever. The USA have already initiated respective standardization activities to promote crypto agility. The European Union should join these nations and take an active part in shaping the future technology landscape. If supported by national and regional governments, this will not only protect economies and the people but create a significant advantage for crypto providers, integrators and enterprise users.





Authors

Dr. Michael Kreutzer
Dr. Ruben Niederhagen
Prof. Dr. Michael Waidner

Authors' address

Fraunhofer SIT
Public Relations
Rheinstrasse 75
64295 Darmstadt
Germany
Telephone +49 6151 869-282
Fax +49 6151 869-224
redaktion@sit.fraunhofer.de

Disclaimer

The contents of this document are the responsibility of Fraunhofer SIT.

Photo credits

Page 11: © Freepik.com
Page 17: © Freepik.com & Fraunhofer SIT
Page 21: © Freepik.com
Page 23: © IBM Research
Others: © Fraunhofer SIT



