Cryptoagility and Quantum Resistance: Easier Said Than Done

Post Quantum Cryptography – The Impact on Identity

Dr. Carmen Kempka

Director Corporate Technology

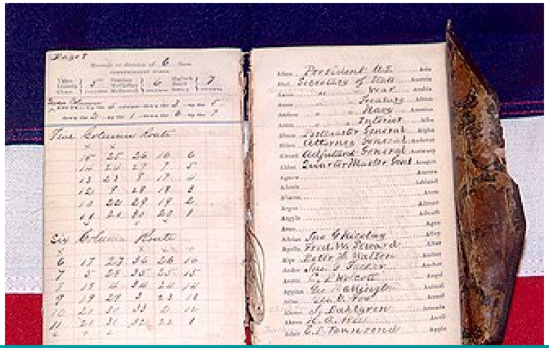
WIBU-SYSTEMS AG

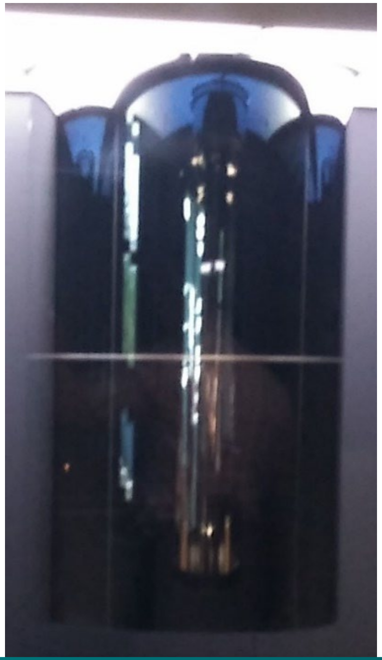
SECURITY
LICENSING
PERFECTION IN PROTECTION

To access the on-demand replay of this masterclass, please visit

https://www.wibu.com/wibu-systems-webinars/post-quantum-cryptography-the-impact-on-identity/access.html

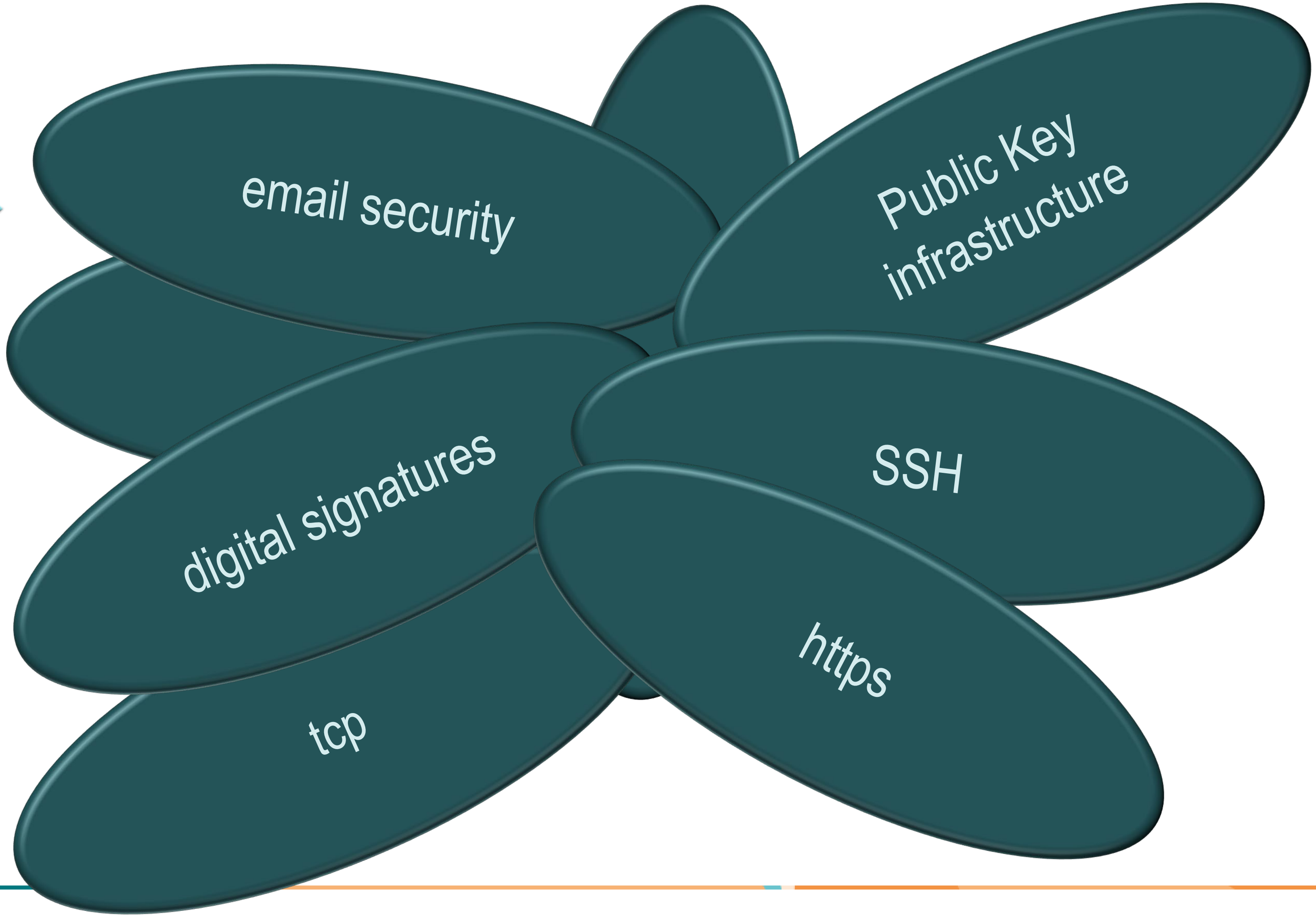
The cat-and-mouse-game of cryptography





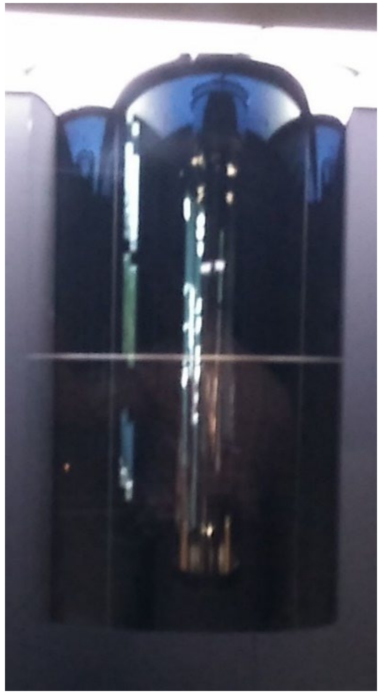
Cryptography develops. So does cryptoanalysis.

Cryptography and quantum computers: What is broken?



Post Quantum Cryptography

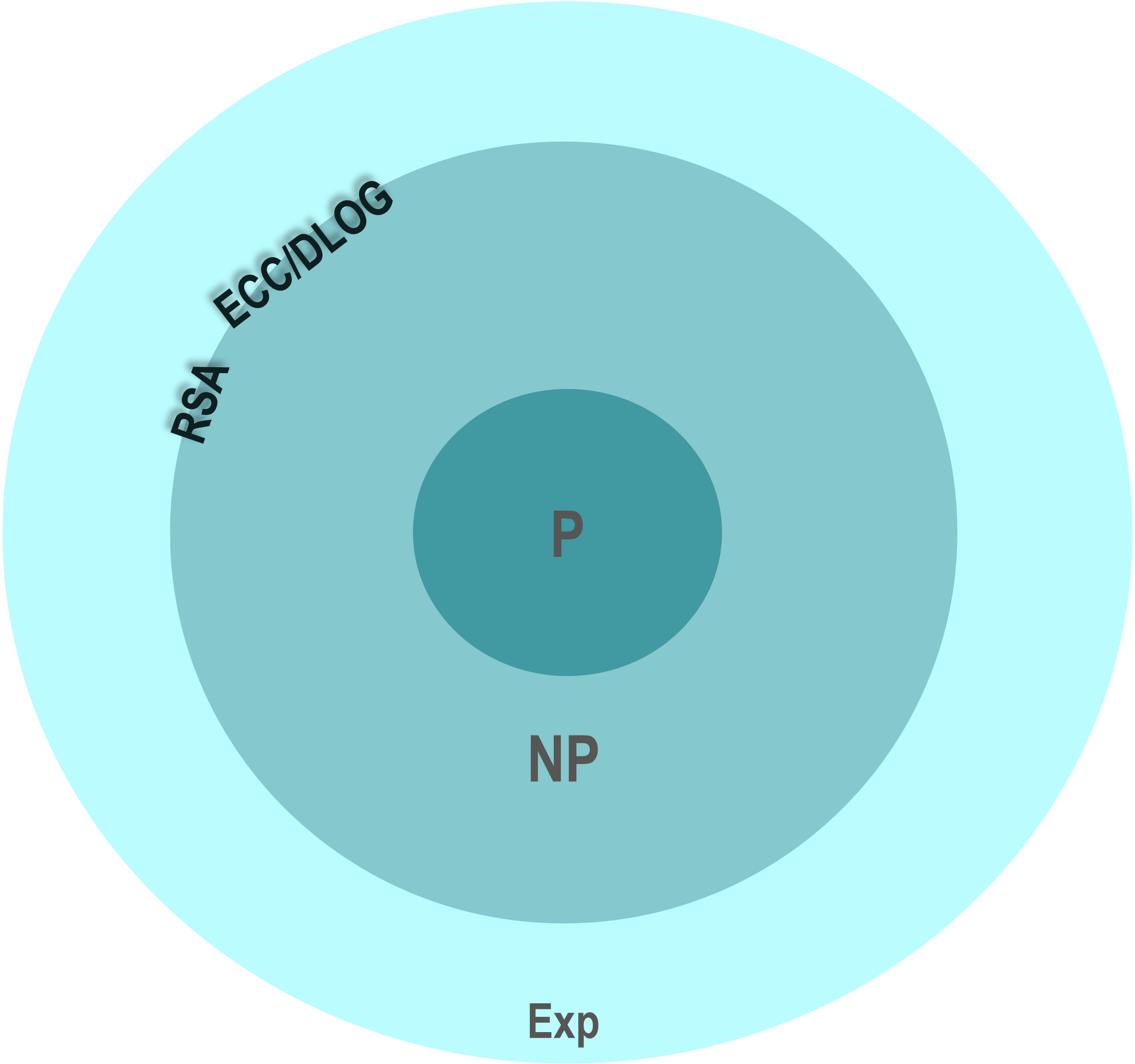
Cryptographic algorithms are resistant against quantum attacks



Asymmetric cryptography

Based on hard mathematical problems

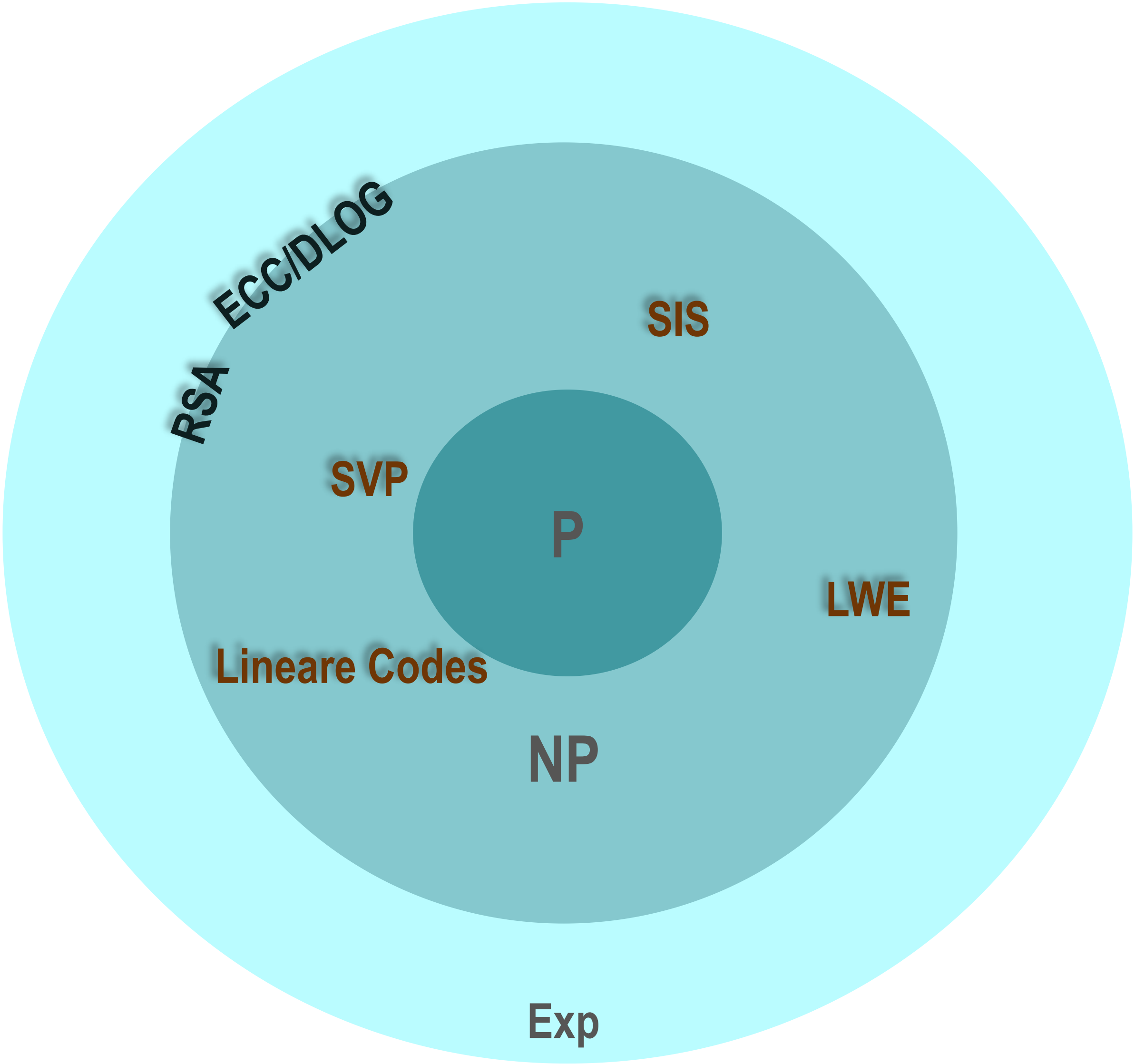
- RSA: factoring large numbers
- ECC: discrete logarithms (DLOG)



Asymmetric cryptography

Based on hard mathematical problems

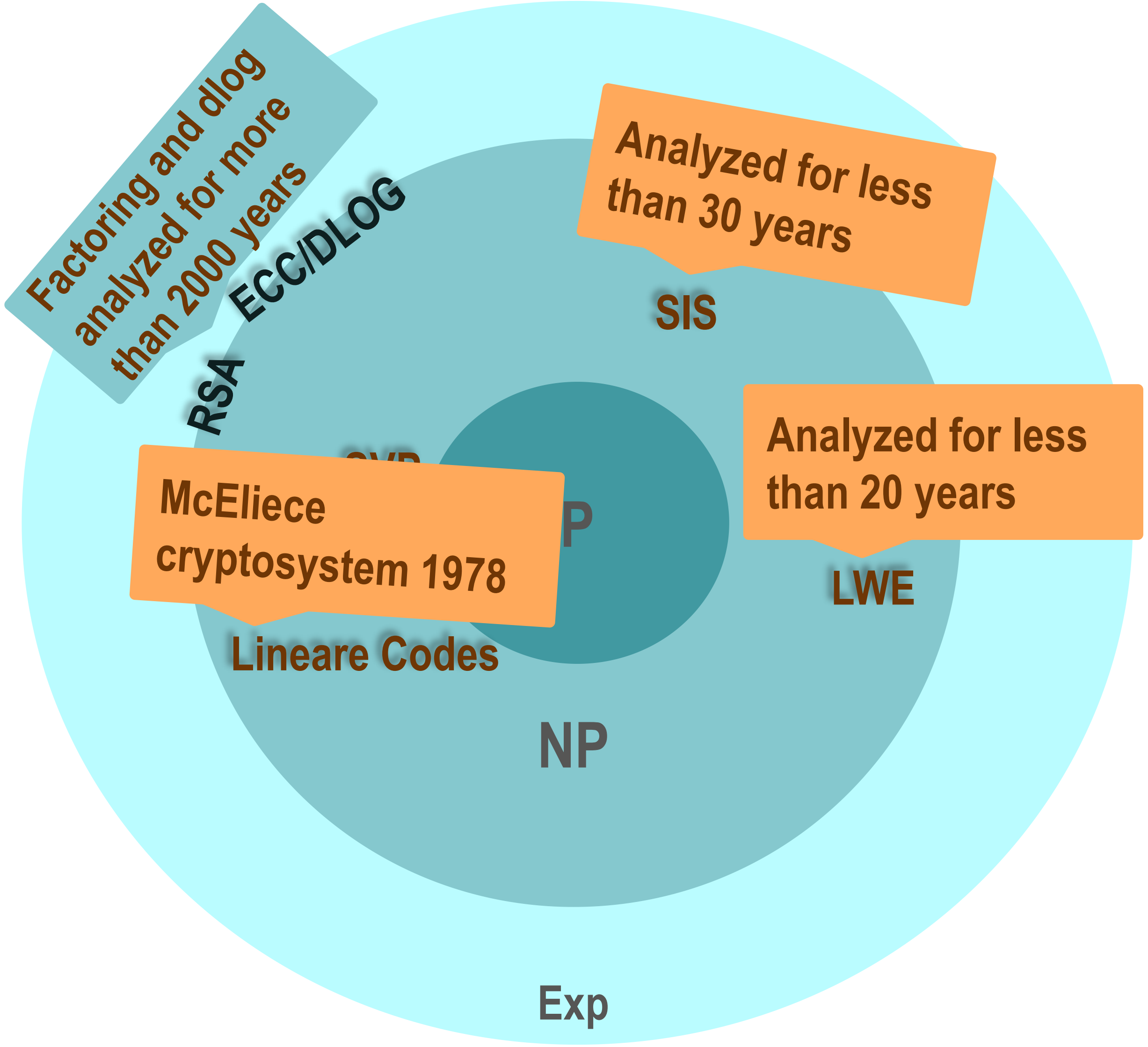
- RSA: factoring large numbers
- ECC: discrete logarithms (DLOG)
- PQC algorithms are based on various, different mathematical problems that are not easily solvable by quantum computers



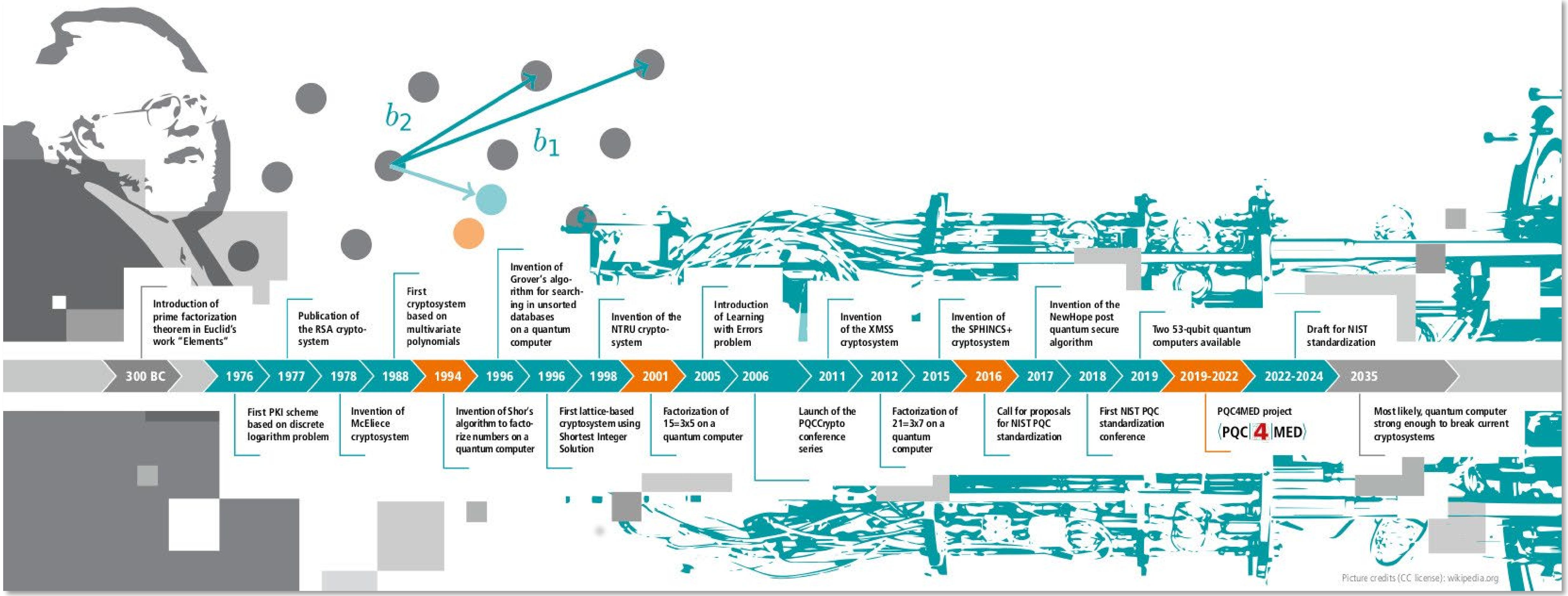
Asymmetric cryptography

Based on hard mathematical problems

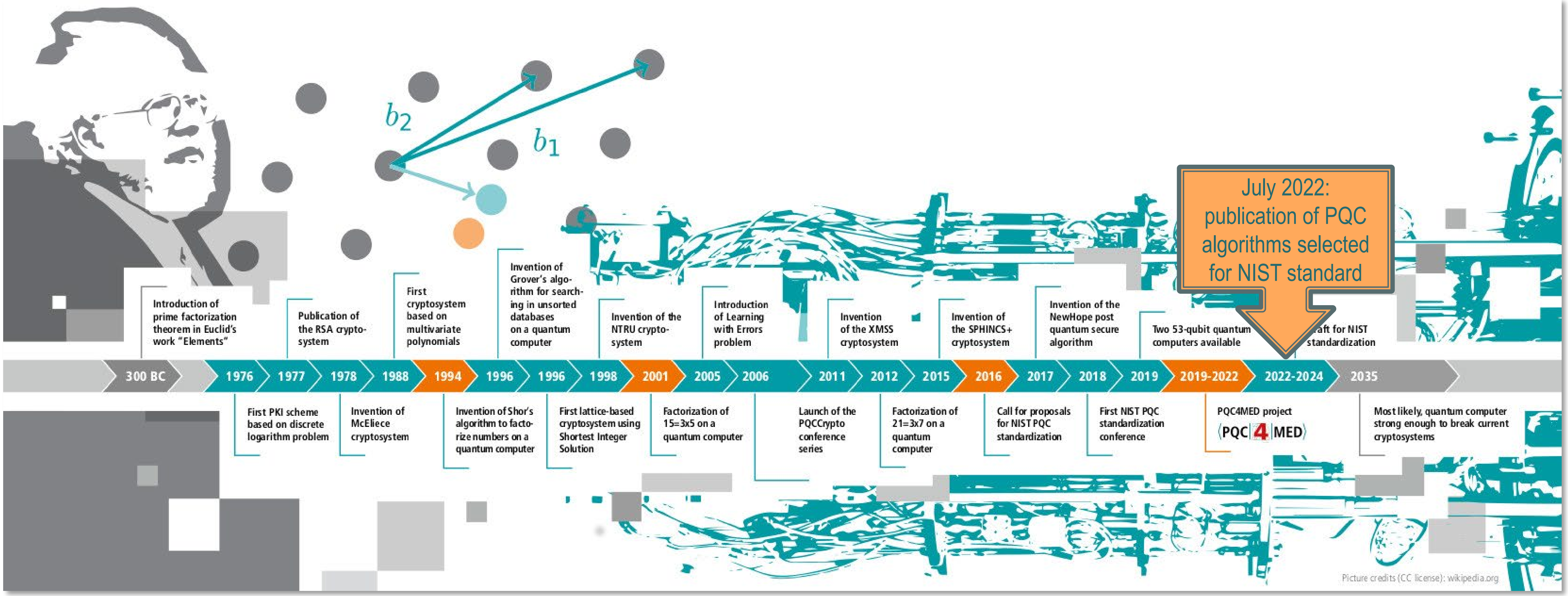
- RSA: factoring large numbers
- ECC: discrete logarithms (DLOG)
- PQC algorithms are based on various mathematical problems that are not easily solvable by quantum computers
- These mathematical problems are much younger and less analyzed!



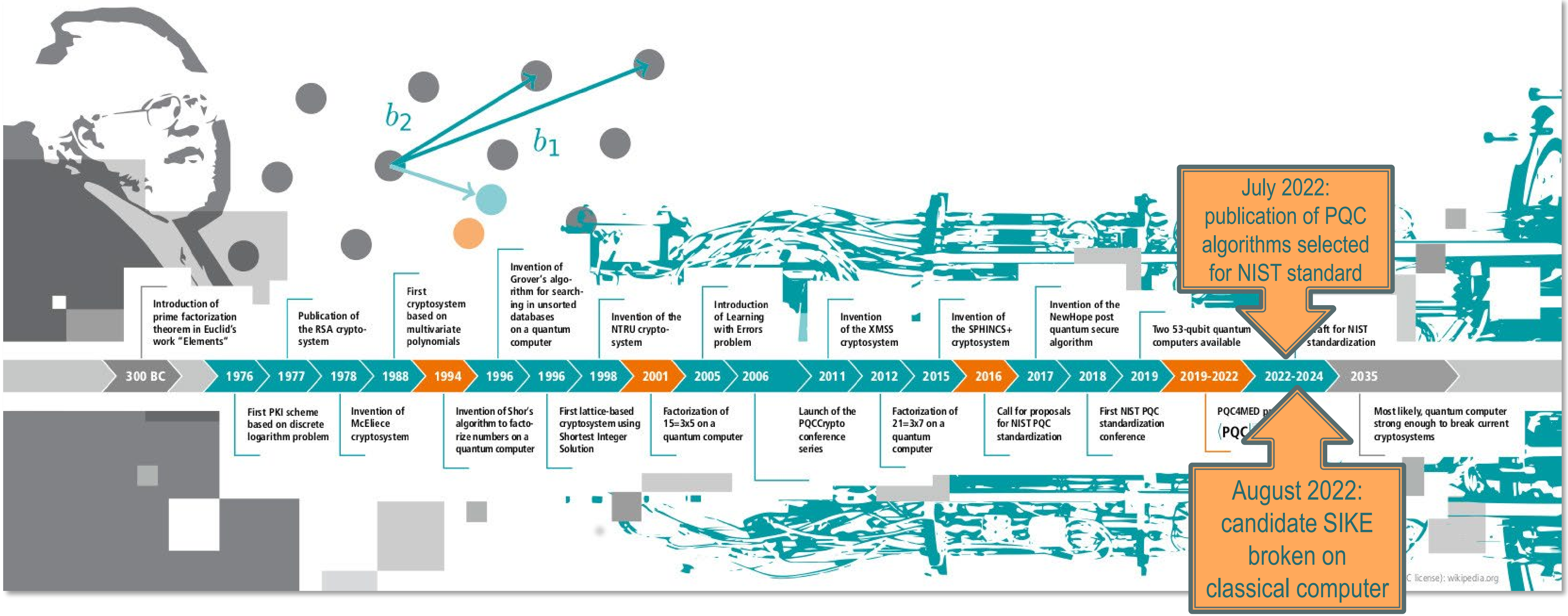
PQC Timeline



PQC Timeline



PQC Timeline

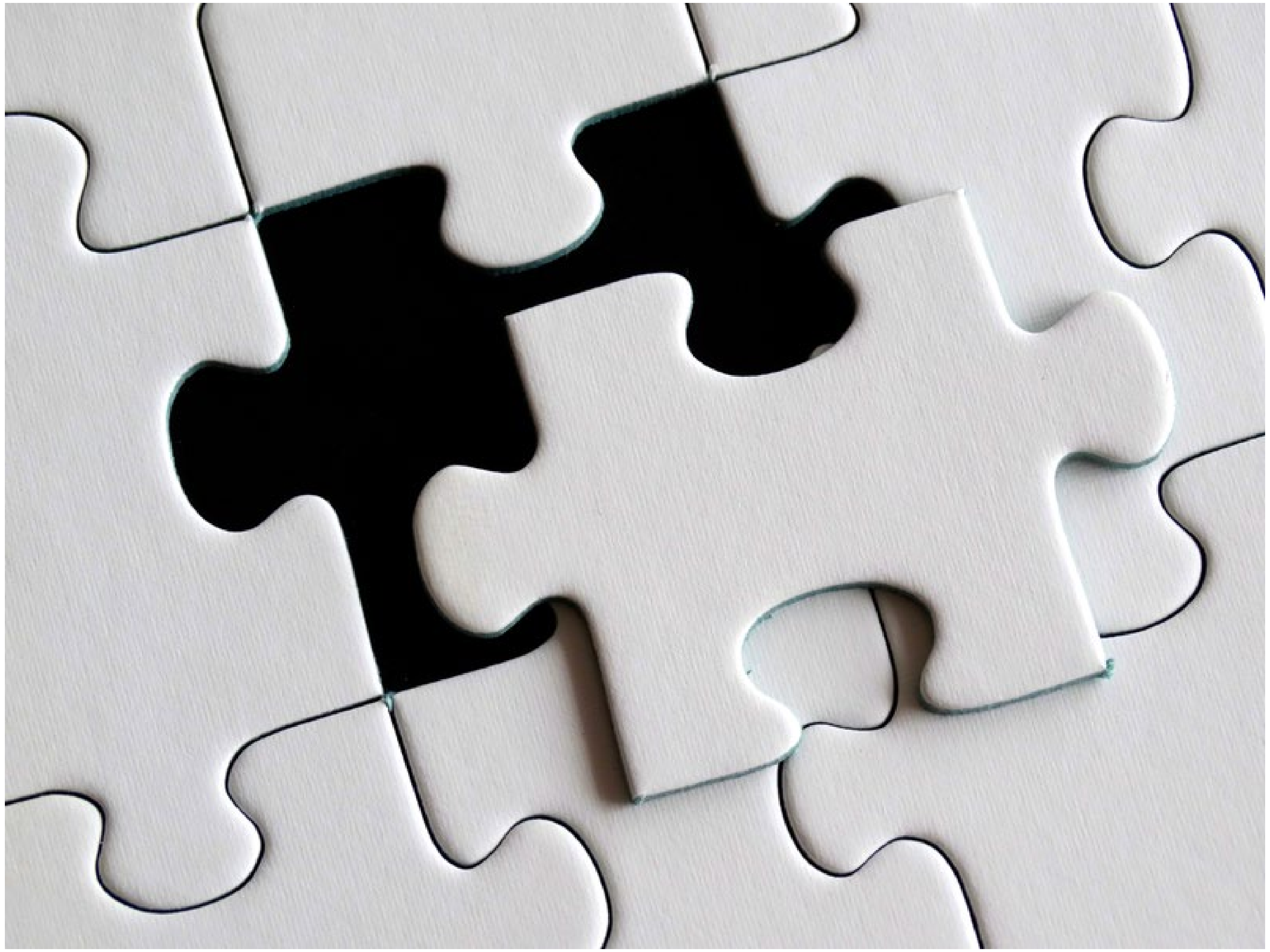


The PQC dilemma

- RSA, ECC:
  - ✓ Factoring and DLOG have been analyzed since around 300 bc (Euclid)
  - ✓ High trust in security against classical attacks
  - – Fully broken with quantum computers – but when?

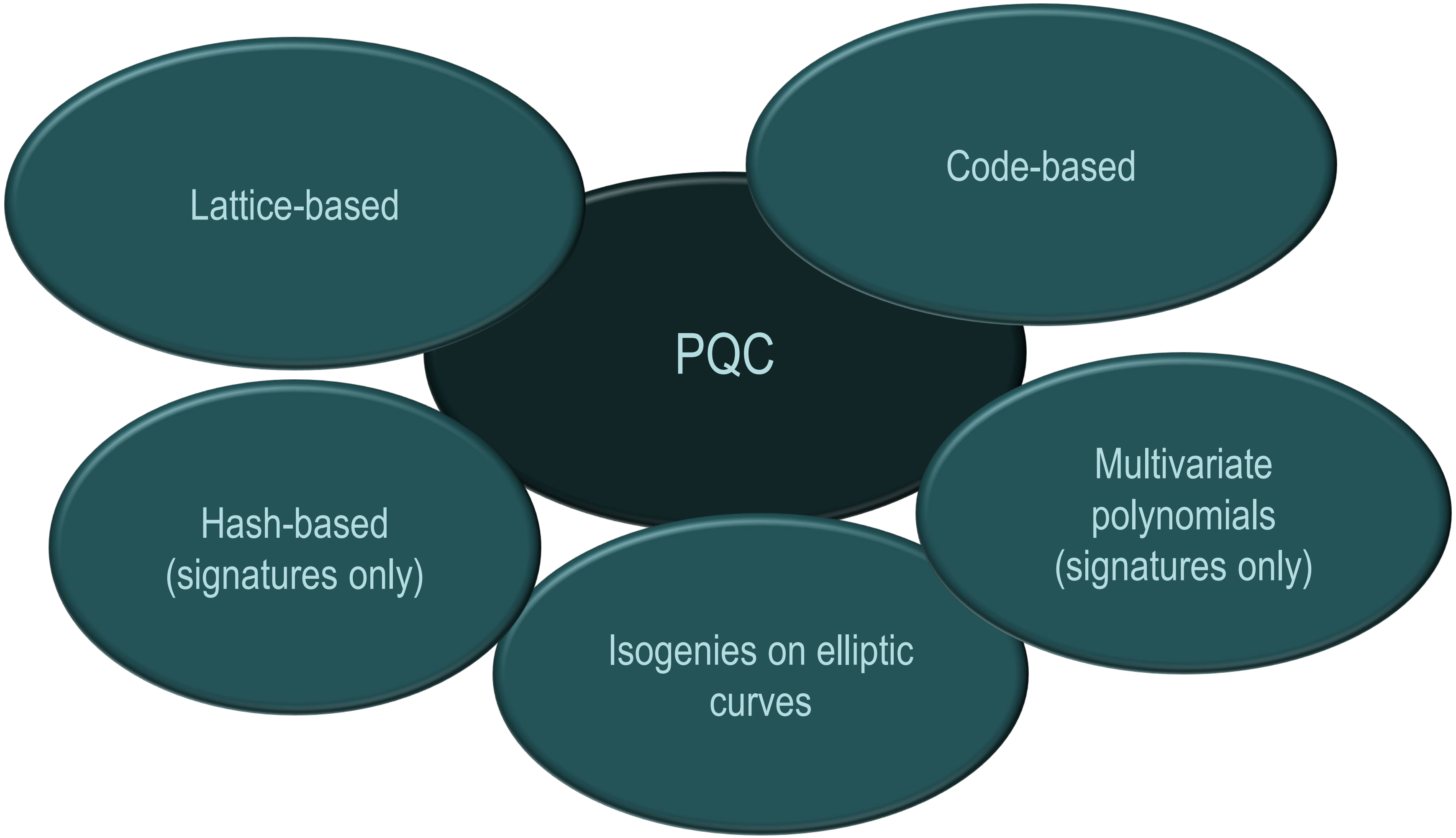
- PQC algorithms
  - Mathematical problems quite new
  - No known relevant attacks by classical or quantum computers
  - Situation hard to assess: not many people have expertise in quantum computers and cryptography or the math behind the PQC schemes

Cryptoagility

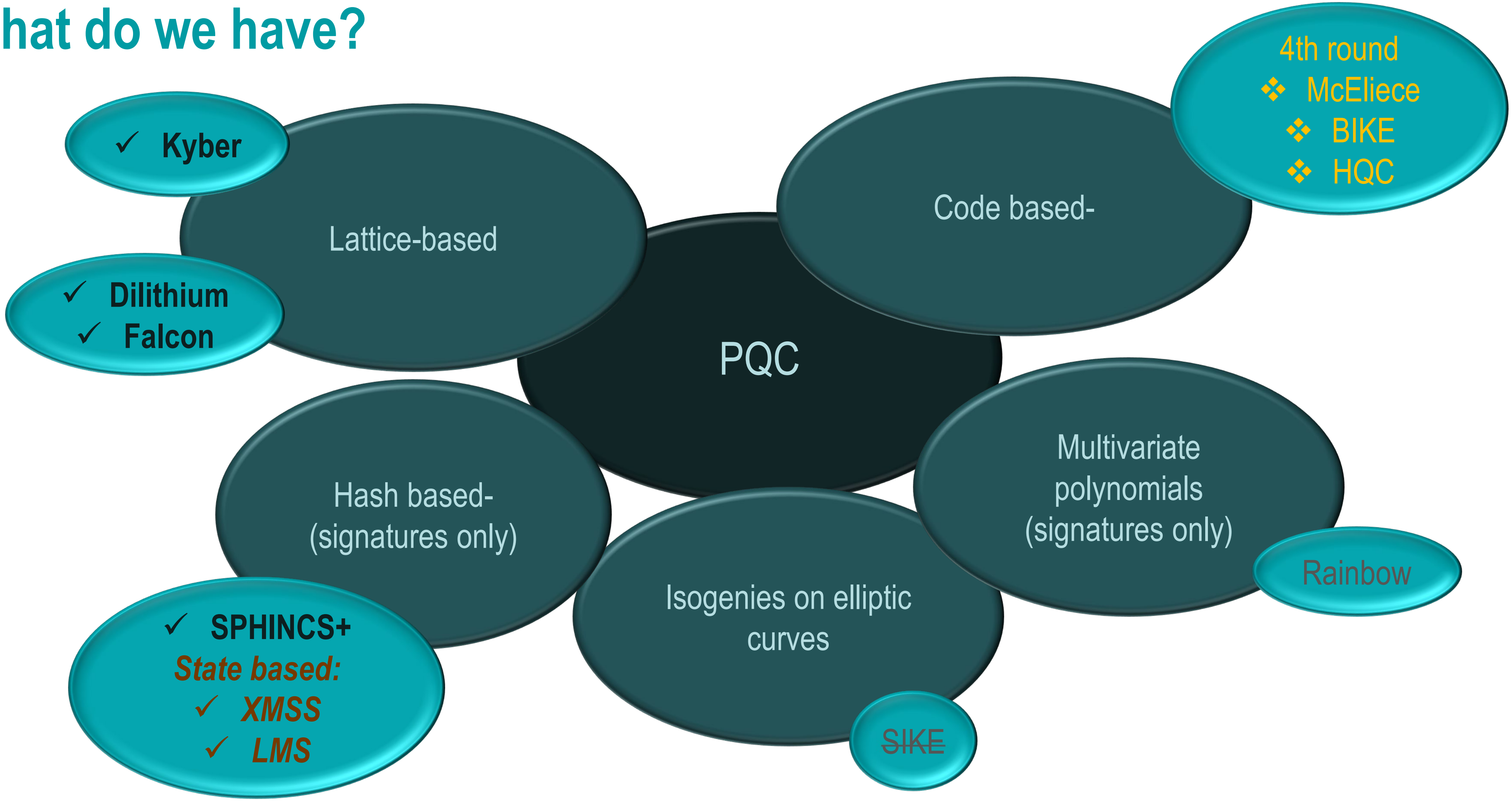


Bildquelle: https://www.goodfreephotos.com/public-domain-images/fitting-the-last-puzzle-piece.jpg.php (Public Domain)

What do we have?



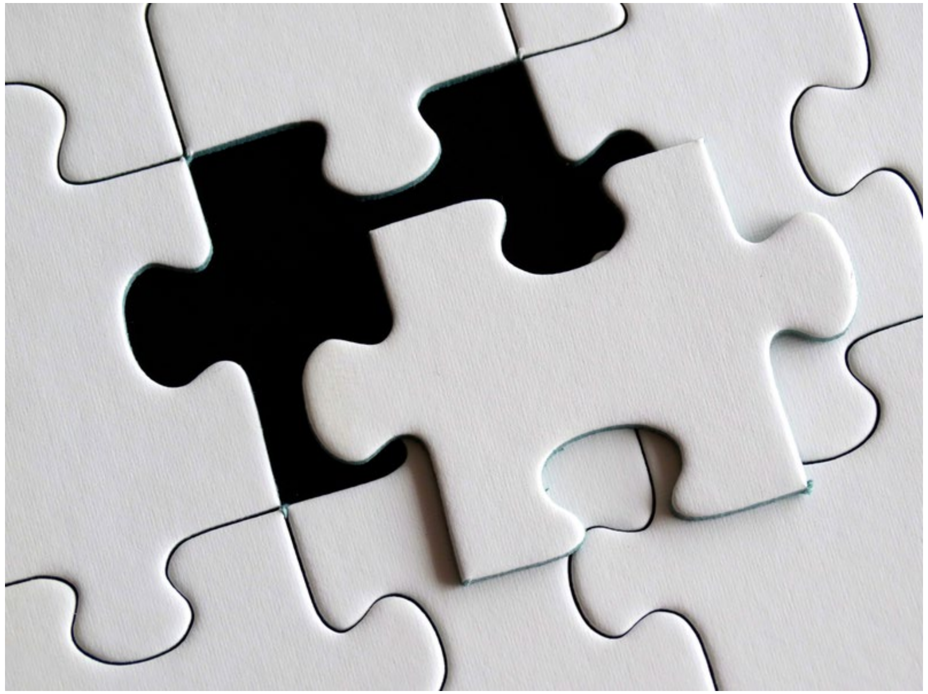
What do we have?



Cryptoagility

The ideal world

```
public abstract class Encryptor {
		abstract String encrypt(int publicKey, String message);
}
public class RSAEncryptor extends Encryptor {
		public String encrypt (int publicKey, String message) {
				<Code for encryption with RSA>
			return ciphertext;
		}
}
public class KyberEncryptor extends Encryptor {
		public String encrypt (int publicKey, String message) {
				<Code for encryption with Kyber>
			return ciphertext;
		}
}
```



Cryptoagility

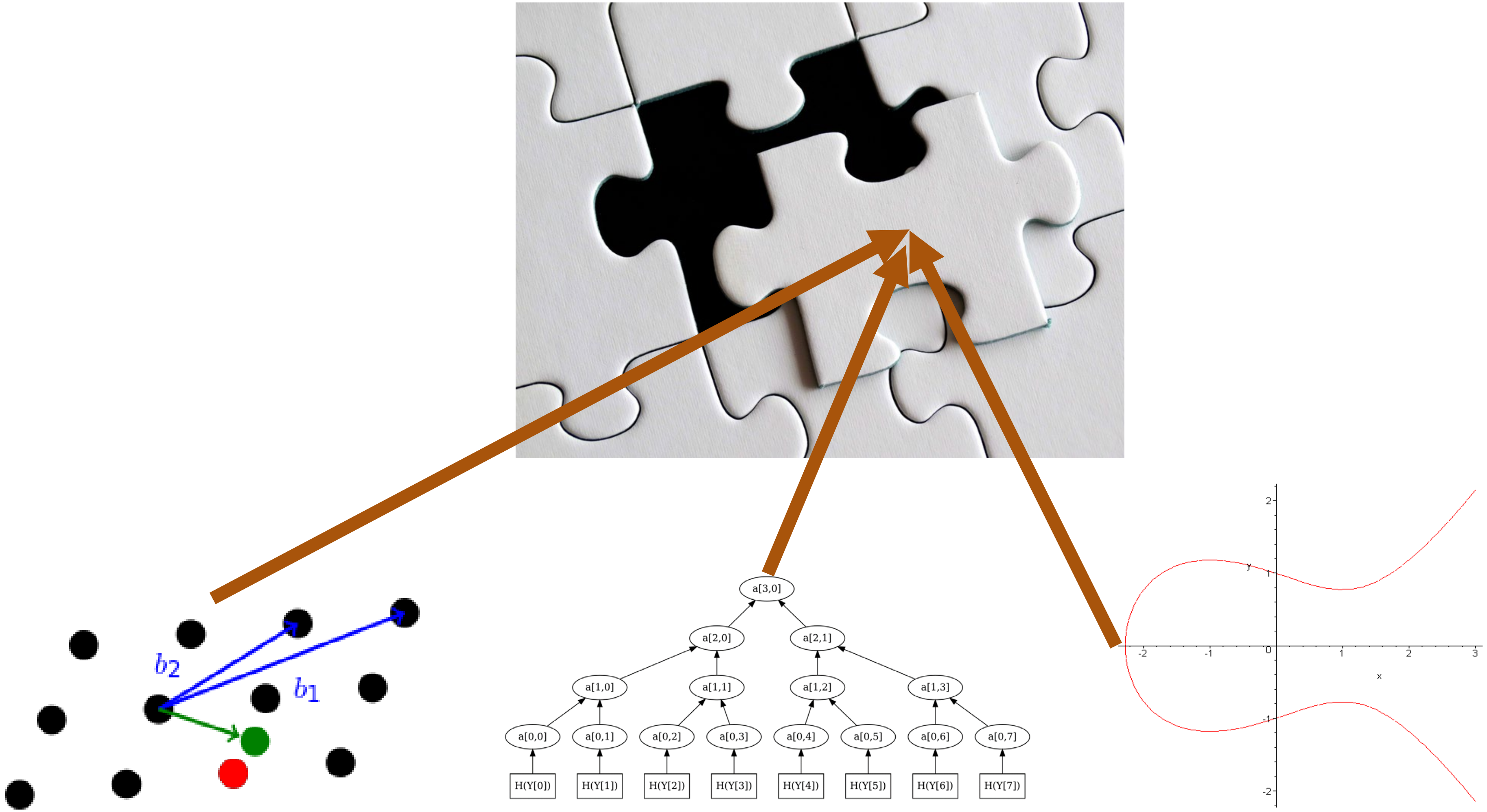
The ideal world

```
public abstract class Encryptor {
		abstract String encrypt(int publicKey, String message);
}
public class RSAEncryptor extends Encryptor {
		public String encrypt (int publicKey, String message) {
			<Code for encryption with RSA>
		return ciphertext;
		}
}
public class KyberEncryptor extends Encryptor {
		public String encrypt (int publicKey, String message) {
			<Code for encryption with Kyber>
		return ciphertext;
		}
}
```

Cryptoagile concept

- Modularity
- Crypto algorithms can be easily replaced if broken
- Once large enough quantum computers exist to break our crypto algorithms, the algorithms are just replaced by PQC algorithms – problem solved

Cryptoagility: the real world



Cryptoagility: easier said than done

- Different mathematical structures
- Large difference in memory requirements
- Very different in performance
- Very different key sizes and formats
- Developers need to learn a lot for each new algorithm
  - Test vectors
  - Formats
  - Memory/performance trade-offs
  - Which intermediate results need to be kept secret
  - How to implement resistance against side channels
  - Other best practices in implementation and usage
  - …

How to deal with cryptoagility

- Plan with enough time and resources
  - management needs to be aware of the full extent of the problem

How to deal with cryptoagility

- Threat analysis
  - Find out where cryptography is used in your system and what is protected against what
  - Maybe use the opportunity to re-asses your security architecture

How to deal with cryptoagility

- Identify memory and performance requirements
  - Hardware requirements
  - Availability requirements of cloud systems
  - Response time
  - Bandwidth
  - …

How to deal with cryptoagility

- Flexibility
  - Restructure code: you need modularity and more flexibility
  - Hardcoded sizes or fixed formats could become a problem
  - Maybe use the opportunity to clean up your code base

How to deal with cryptoagility

- Get experience
  - Try out open source PQC libs to identify performance issues etc.
  - Do research projects

How long do we have time?

When should we start integrating quantum resistant cryptography?

Mosca's Theorem

When should we start?

Let…

…X the time for which encryption should be secure

…Y the time needed for migrating to PQC

…Z the time remaining until quantum computers are sufficiently advanced to break current cryptographic systems

Theorem (Mosca):

If X + Y > Z, then worry

Source Mosca's Theorem: https://csrc.nist.gov/csrc/media/events/workshop-on-cybersecurity-in-a-post-quantum-world/documents/presentations/session8-mosca-michele.pdf

Mosca's Theorem

When should we start?

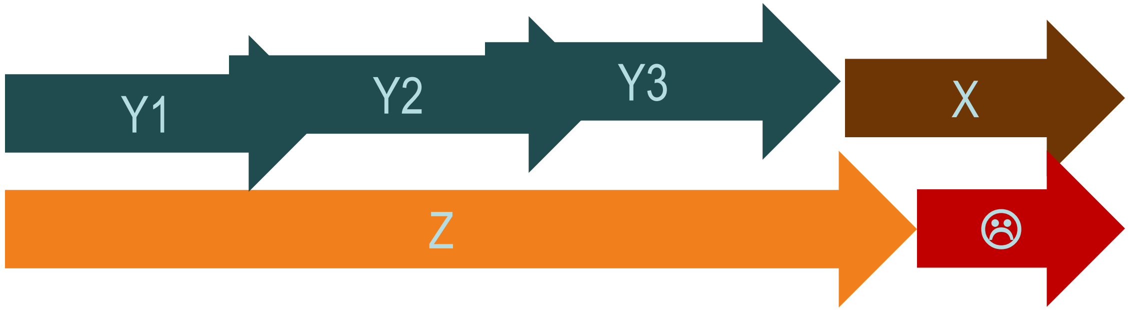
Let…

…X the time for which encryption should be secure

…{Y1..Yn} the time needed for migrating the entire value chain to PQC

…Z the time remaining until quantum computers are sufficiently advanced to break current cryptographic systems

Theorem:



If X + Y > Z, then worry

When do quantum computers start becoming dangerous

We don’t know that.

- Needed to break ECC 256: around 2330 logical qubits or several million physical qubits
- Needed to break RSA 2048: around 4096 logical qubits or several million physical qubits
- Currently existing quantum computers have a few hundred physical qubits

Seems we are still far away from having our crypto systems broken, but

everything between < 10 and > 30 years is possible

Migration to PQC

- Long-term security: combination of different algorithms
  - Hybrid certificates
  - Double encryption
- Cryptoagility
  - Where is cryptography used in your system?
  - Make cryptography updatable and replaceable
- Find a good strategy for the transition
  - Identify dependencies
  - Coordinate migration to PQC with suppliers and customers
  - Requirements of downwards compatibility and interoperability

Thank You!

Let’s keep in touch

Europe: +49-721-931720

USA: +1-425-7756900

China: +86-21-55661790

Japan: +81-45-5659710

https://www.wibu.com

info@wibu.com