When will the quantum computer age start?

Quantum Computers and Cryptography
Small-scale quantum computers have already been created by large companies and organizations around the world. These computers are expanding rapidly, and the goal of a large-scale quantum computer seems within reach in the not-too-distant future.

When these computers become available, current public-key cryptosystems like RSA or elliptic curves will become insecure. Shor’s algorithm shows how, using a quantum computer, the prime factorization of a large number and the calculation of discrete logarithms can be done in polynomial time.

Additionally, symmetric encryption algorithms and hash functions that are not directly tied to a mathematical problem are also at risk, as Grover’s algorithm shows. In this case, the impact is not as devastating as in public-key cryptography, but the time it takes to break a symmetric scheme or a hash function through a brute-force attack or an exhaustive search is reduced by almost half.

The probability to break RSA 2048 by 2031 is estimated at 50%. Complex software solutions and products usually entail long and arduous product development processes. Additionally, many industries like automotive, aerospace, transportation, public and critical infrastructure, design and produce goods today that will be on the market for the next 20 to 50 years.

Who is affected
The probability to break RSA 2048 by 2031 is estimated at 50%. Complex software solutions and products usually entail long and arduous product development processes. Additionally, many industries like automotive, aerospace, transportation, public and critical infrastructure, design and produce goods today that will be on the market for the next 20 to 50 years.

Another interesting aspect of these industries is their reliance on pre-orders that are produced now, but delivered far off in the future (+10 years). These products will most certainly face the threat of quantum computers. Consequently, it is essential to plan ahead and integrate the required protection mechanisms in the design and production processes that take place today.

Type | Algorithm | Key Strength Classic (bits) | Key Strength Quantum (bits) | Quantum Attack |
--- | --- | --- | --- | --- |
Asymmetric | RSA 2048 | 112 | 0 | Shor’s Algorithm |
| RSA 3072 | 128 | | |
| ECC 256 | 128 | | |
| ECC 512 | 256 | | |
| Symmetric | AES 128 | 128 | 64 | Grover’s Algorithm |
| AES 256 | 256 | 128 | |

Source: iseara.com

The probability to break RSA 2048 by the year 2031 is estimated at 50 percent.
MTG Post-Quantum Cryptography (MTG PQC)

Protect current systems against future quantum computer threats

**Public Key Infrastructure – PQC PKI**

**Use cases**
- Corporate PKI
- General Purpose PKI
- Health/Insurance PKI
- Government PKI
- IoT PKI
- e-Energy PKI

**Short description & features**
- MTG-CARA is a flexible, configurable, multi-tenant CA for the generation and administration of certificates using traditional and post-quantum cryptography (PQC)
- Certification and Registration Authority
- Supports standardized interfaces such as SOAP, SCEP, LDAP and OCSP
- Generation and management of X.509, AC, Card Verifiable (CV) certificates
- Modular design allows fast, low-cost customizing
- Special rights and roles concept to map individual organizational structure
- Support for software/chip card/network-HSM signing
- Scalable from a single-server solution up to the operation of a large scale CA

**MTG Key Management System – PQC KMS**

**Use cases**
- Production & operation of IoT Devices (e.g. Smart Meters)
- Central Management of ERP-systems

**Short description & features**
- Highly available management of traditional and PQC keys for various applications
- Detached, central security module, able to perform all necessary cryptographic operations
- Multi-tenant architecture
- Fine-granular rights management
- Management of the entire life cycle of keys
- Standardized KMIP interface v1.4
- HSM support for multiple vendors

**PQC HSM Integration**

**Use cases**
- Strong protection and use of PQC keys is necessary
- Compliance with industry standards is mandatory
- A customised hardware solution is required to use proprietary formats or workflows, for example

**Short description**
- Integration of PQC algorithms in HSMs
- Extension Module can be added to already deployed HSMs
- Developed with UTIMACO SDK
- Seemless integration of PQC into existing customer applications and products by leading PQC experts
- Mitigation of risks in transition phase

**PQC Suite**

**Use cases**
- Web Server & Client
- Email Communication
- Document Signing
- Document Encryption

**Examples:**
- Registration Portals
- Credentials over the Web
- Transfer of personal data
- E-Banking
- Handling of confidential documents

**Short description**
- Migration of business applications, products, custom protocols to PQC
- Insight in dealing with large keys and signatures
- Efficient implementations of PQC algorithms
- Mitigation of risks in transition phase

**PQC Services**

**Use cases**
- PQC Web Server: based on Apache Tomcat, offers all the features of a modern web server with integrated support for PQC TLS
- PQC Web Browser: based on Mozilla Firefox, offers all the features of a modern browser with integrated support for PQC TLS
- PQC Email Client: based on Mozilla Thunderbird, offers all the features of a modern email client with integrated support for PQC S/MIME
- Document Signing: Solution for generic document signing and encryption using state of the art PQC algorithms
**MTG Post-Quantum Cryptography (MTG PQC)**

Protect current systems against future quantum computer threats

### Public Key Infrastructure – PQC PKI

**Use cases**
- Corporate PKI
- General Purpose PKI
- Health/Insurance PKI
- Government PKI
- IoT PKI
- e-Energy PKI

<table>
<thead>
<tr>
<th>Certification Request and Registration</th>
<th>Approval / Disapproval</th>
<th>Revocation Request</th>
<th>Configuration and Management</th>
</tr>
</thead>
</table>

**MTG-CARA**
- Certificate issuance
- Creation of Revocation Lists
- Central Logging
- Authorisation

- Smartcard production and personalisation
- E-Mail notification and delivery
- Publication and Directory Services
- Revocation lists
- Billing
- Expert, Static, Archive

**Short description & features**
- MTG-CARA is a flexible, configurable, multi-tenant CA for the generation and administration of certificates using traditional and post-quantum cryptography (PQC)
- Certification and Registration Authority
- Supports standardized interfaces such as SOAP, SCEP, LDAP and OCSP
- Generation and management of X.509, AC, Card Verifiable (CV) certificates
- Modular design allows fast, low-cost customizing
- Special rights and roles concept to map individual organizational structure
- Support for software/chip card/network-HSM signing
- Scalable from a single-server solution up to the operation of a large scale CA

### MTG Key Management System – PQC KMS

**Use cases**
- Production & operation of IoT Devices (e.g. Smart Meters)
- Central Management of ERP-systems

**Short description & features**
- Highly available management of traditional and PQC keys for various applications
- Detached, central security module, able to perform all necessary cryptographic operations
- Multi-tenant architecture
- Fine-granular rights management
- Management of the entire life cycle of keys
- Standardized KMIP interface v1.4
- HSM support for multiple vendors

**KMIP – Key Management Interoperability Protocol**
- Key & Certificate Life Cycle Management
- Attributes / Metadata
- Cryptographic Services
- Authentication
- Audit / Reporting
- Policy Standard Compliance

**HSM-Interface**

### PQC HSM Integration

**Use cases**
- Strong protection and use of PQC keys is necessary
- Compliance with industry standards is mandatory
- A customised hardware solution is required to use proprietary formats or workflows, for example

**Short description**
- Integration of PQC algorithms in HSMs
- Extension Module can be added to already deployed HSMs
- Developed with UTIMACO SDK
- Seamlessly integrates PQC into existing customer applications and products by leading PQC experts
- Mitigation of risks in transition phase

**Examples:**
- Registration Portals
- Credentials over the Web
- Transfer of personal data
- E-Banking
- Handling of confidential documents

### PQC Suite

**Use cases**
- Where long term security is needed in:
- Web Server & Client
- Email Communication
- Document Signing
- Document Encryption

**Examples:**
- Registration Portals
- Credentials over the Web
- Transfer of personal data
- E-Banking
- Handling of confidential documents

**Short description**
- Migration of business applications, products, custom protocols to PQC
- Insight in dealing with large keys and signatures
- Efficient implementations of PQC algorithms
- Mitigation of risks in transition phase

**Examples:**
- PQC Web Server: based on Apache Tomcat, offers all the features of a modern web server with integrated support for PQC TLS
- PQC Web Browser: based on Mozilla Firefox, offers all the features of a modern browser with integrated support for PQC TLS
- PQC Email Client: based on Mozilla Thunderbird, offers all the features of a modern email client with integrated support for PQC S/MIME
- Document Signing: Solution for generic document signing and encryption using state of the art PQC algorithms

### PKC Services

**Use cases**
- Migration of business applications, products, custom protocols to PQC
- Insight in dealing with large keys and signatures
- Efficient implementations of PQC algorithms
- Mitigation of risks in transition phase

**Short description**
- Seamsless integration of PQC into existing customer applications and products by leading PQC experts
- In close cooperation with our customers, we integrate PQC into existing applications and protocols in joint projects
- Hardware and software optimisations
- Hybrid schemes which benefit from both universes: tried and tested crypto methods (such as RSA or ECC) combined with new quantum-safe methods
Quantum Computers and Cryptography

Small-scale quantum computers have already been created by large companies and organizations around the world. These computers are expanding rapidly, and the goal of a large-scale quantum computer seems within reach in the not-too-distant future.

When these computers become available, current public-key cryptosystems like RSA or elliptic curves will become insecure. Shor's algorithm shows how, using a quantum computer, the prime factorisation of a large number and the calculation of discrete logarithms can be done in polynomial time.

Additionally, symmetric encryption algorithms and hash functions that are not directly tied to a mathematical problem are also at risk, as Grover's algorithm shows. In this case, the impact is not as devastating as in public-key cryptography, but the time it takes to break a symmetric scheme or a hash function through a brute-force attack or an exhaustive search is reduced by almost half.

<table>
<thead>
<tr>
<th>Type</th>
<th>Algorithm</th>
<th>Key Strength Classic (bits)</th>
<th>Key Strength Quantum (bits)</th>
<th>Quantum Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asymmetric</td>
<td>RSA 2048</td>
<td>112</td>
<td>0</td>
<td>Shor's Algorithm</td>
</tr>
<tr>
<td></td>
<td>RSA 3072</td>
<td>128</td>
<td>0</td>
<td>Shor's Algorithm</td>
</tr>
<tr>
<td></td>
<td>ECC256</td>
<td>128</td>
<td>0</td>
<td>Shor's Algorithm</td>
</tr>
<tr>
<td></td>
<td>ECC521</td>
<td>256</td>
<td>0</td>
<td>Grover's Algorithm</td>
</tr>
<tr>
<td></td>
<td>AES128</td>
<td>128</td>
<td>64</td>
<td>Grover's Algorithm</td>
</tr>
<tr>
<td></td>
<td>AES 256</td>
<td>256</td>
<td>128</td>
<td>Grover's Algorithm</td>
</tr>
</tbody>
</table>

Another interesting aspect of these industries is their reliance on pre-orders that are produced now, but delivered far off in the future (+10 years). These products will most certainly face the threat of quantum computers. Consequently, it is essential to plan ahead and integrate the required protection mechanisms in the design and production processes that take place today.

The probability to break RSA 2048 by the year 2031 is estimated at 50 percent.

The protection of your data against future decryption by quantum computers is already possible today with our PQC portfolio. To this end, we have developed a new generation of MTG products which allow the seamless integration of PQC algorithms.

Anyone developing long-lived products or who is responsible for highly sensible data should start getting to grips with PQC today!