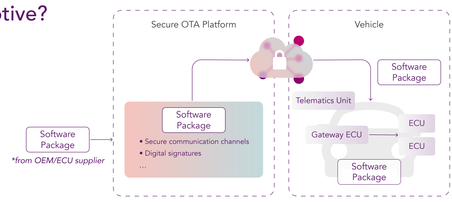
Automotive security and quantum computing

Quantum Computing (QC) represents one of the biggest threats to security in the medium term since it can make attacks against cryptography much more efficient. QC capabilities are advancing from the realm of academic exploration to tangible commercial opportunities. Therefore, now is the time to take steps to secure everything from power grids and IoT infrastructures to the growing cloud-based information-sharing platforms that we are all increasingly dependent upon.

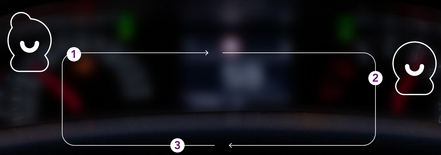
How is cryptography used in automotive?

With new regulations coming in place in 2024, cryptography has become the backbone for cybersecurity implementation in the automotive industry. A practical example of a standard cryptography practice in automotive is Over-The-Air (OTA), where updates are transmitted to only the authorized and authenticated software installed on a vehicle's control units. This helps prevent unauthorized modifications that could compromise vehicle safety and performance.



HOW PUBLIC-KEY CRYPTOGRAPHY WORKS

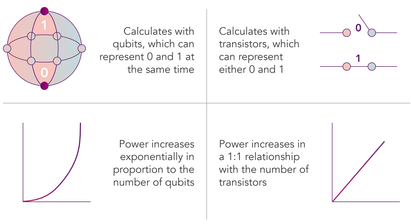
Alice sends her **public key** to Bob. This works like an open padlock. Anyone can use it to encrypt information, but only the **matching private key** can unlock it.



Bob uses Alice's public key to encrypt his message. He sends this encoded message to Alice.

Alice uses her **private key** - which hasn't been shared with anyone - to decrypt Bob's message. Unless the private key has been compromised, no one but her can read the contens.

QUANTUM COMPUTING VS CLASSICAL COMPUTING



What is the quantum threat to cybersecurity?

The rapid advancements in quantum computing pose a significant threat to traditional cryptographic systems as it can solve the problems far more efficiently than standard computers, potentially rendering many of today's cryptographic systems insecure. With the potential to break the current widely used encryption protocols, such as RSA and Elliptic Curve Cryptography, the need to prepare for post-quantum cryptography has never been more crucial.

EVOLUTION OF CRYPTOGRAPHIC ALGORITHMS

1970s-2000s — DES

- US National Bureau of Standards launched the Data Encryption Standard (DES)

1990s-2010s — 3DES

- Triple DES (3DES) uses three 56-bit keys. It works on a block of data by splitting it in two and iteratively applying arbitrary round functions derived from an initial function

2000s-present — AES & ECC

- Advanced Encryption Standard (AES), with 128-, 192-, or 256-bit keys
- AES encryption has completely replaced DES worldwide as the default symmetric encryption cipher used for public and commercial purposes
- ECC is an approach to encryption that utilizes the complex nature of elliptic curves in finite fields

2000s-present — RSA

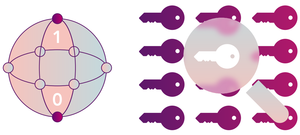
- RSA encryption utilizes the property of complexity classes wherein the problem of prime integer factorization lies inside the non-polynomial time (NP- hard) class

2030s — Quantum Computing

- Post-quantum cryptography methods include lattice-based, code-based, hash-based, isogeny-based, and multivariate systems Encryption Methods

Why plan now for security in the quantum era?

Within the next decade, computing power and stability of quantum machines are expected to reach a level where they can render current public key encryption protocols vulnerable. This presents a grave concern for the protection of sensitive data, applications and transactions that we rely on daily. Moreover, bad actors are already collecting data with the intention of decrypting it once quantum computers become capable – a tactic known as the 'harvest now, decrypt later' threat.



WHAT HAPPENS NEXT AND HOW CAN IRDETO HELP?

Irdeto is part of an EU funded project called Together for RISc-V Technology and Applications (TRISTAN), a Key Digital Technologies Joint Undertaking within the Horizon Europe funding program. The overarching goal of TRISTAN is to expand, mature and industrialize the European RISc-V ecosystem to compete more effectively with existing commercial alternatives.

Within TRISTAN, Irdeto will collaborate with partners in the Dutch sector of the consortium to architect, design and implement new secure root-of-trust, secure boot and firmware update mechanisms that employ Post Quantum Cryptography (PQC) algorithms. With this and other industry driven projects, Irdeto is building the capacity and preparing for future attacks (based on the usage of quantum computers) by transitioning to PQC, while gaining expertise on how to implement these algorithms.

irdeto

At Irdeto we have strong automotive industry knowledge and understanding combined with more than 50 years of embedded cybersecurity expertise. We secure over six billion devices and applications around the world. In addition to automotive, our security solutions are used across a wide variety of industries and businesses from video entertainment, gaming and broadcast to construction, industrial manufacturing and healthcare.