Post-quantum cryptography in the automotive industry

escrypt

SECURITY. TRUST. SUCCESS.

Post-quantum cryptography in the automotive industry

Presenter

Dr. Yousik Lee

- PhD (Information Security)
- Director
- Chief Information Security Officer
- Lead cybersecurity business in KOREA
- +22 years IT, +17 years CS, +10 years automotive CS experiences
- ITU-T SG17 delegate of KOREA
- TTA PG504 committee member
- Korea Cryptography Forum committee member

ETAS GmbH

- Parent company: Robert Bosch GmbH (100% subsidiary of the Bosch Group)
- Year of establishment: 1994
- Number of Employees: About 1,500 (2021)
- Sales: 321.5 million euros (2021)
- Locations: 31 branches/offices in 12 countries
- ESCRYPT, cybersecurity brand

Post-quantum cryptography in the automotive industry

Agenda

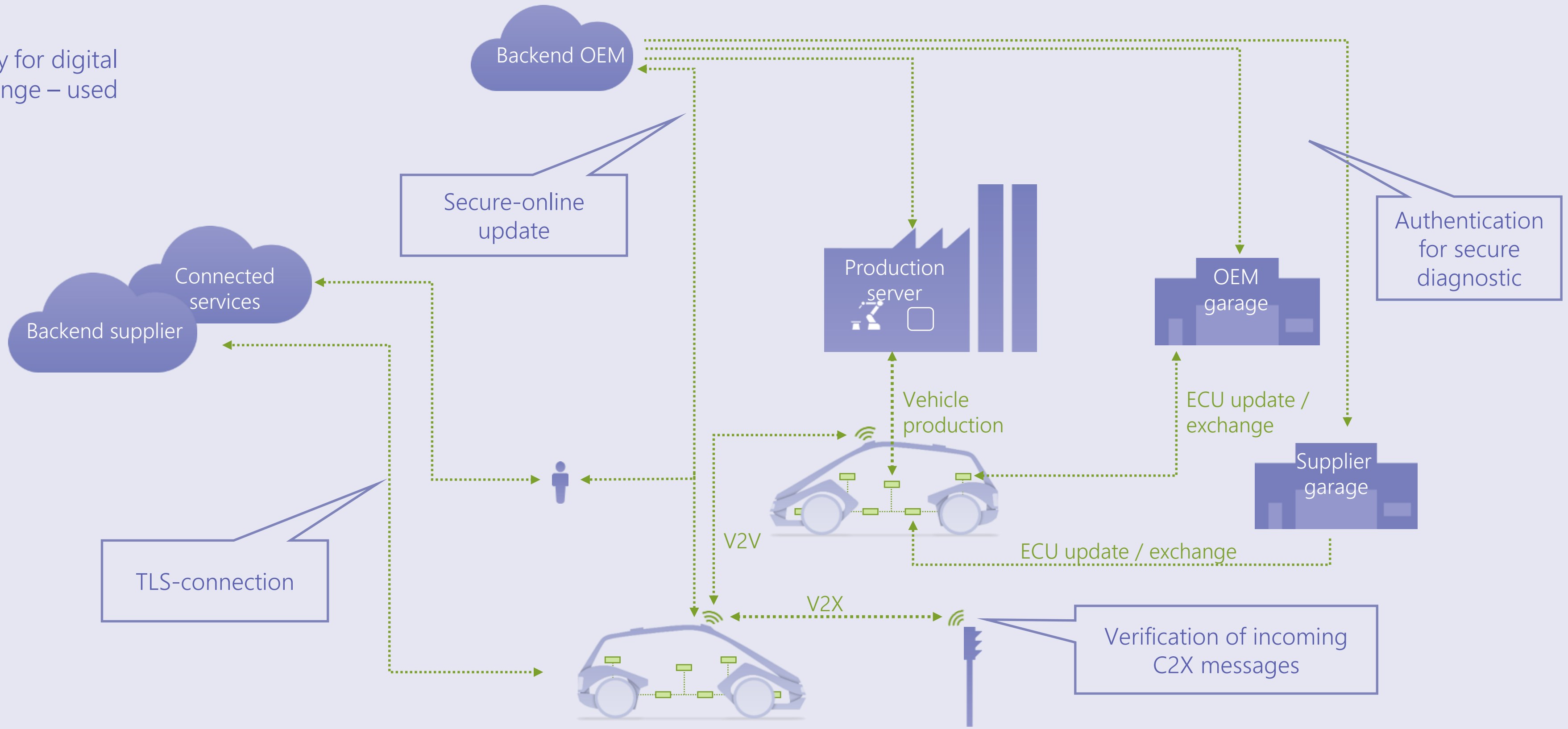
1. Introduction & motivation
2. Quantum computers and post-quantum algorithms
3. Challenges for the automotive industry
4. Summary

Introduction & motivation

Introduction and motivation

Example communication flow for an average future car

Asymmetric cryptography for digital signatures and key exchange – used today RSA and ECC



Backend OEM

Secure-online update

Connected services

Backend supplier

Production server

OEM garage

Authentication for secure diagnostic

Vehicle production

ECU update / exchange

Supplier garage

V2V

ECU update / exchange

TLS-connection

V2X

Verification of incoming C2X messages

Flow of cryptographic information/material

Quantum computers and post-quantum algorithms

Quantum computers and post-quantum algorithms

A story of Bits and Qubits

- **Quantum computer** leverages quantum mechanical phenomena, such as quantum entanglement and superposition in order to perform computations
- Any problem that QC can solve, can be solved by classical computers – given enough time! It is however assumed, that quantum supremacy can be achieved, i.e. using a quantum computer to solve a problem that cannot be solved by a classical computer in any feasible amount of time.

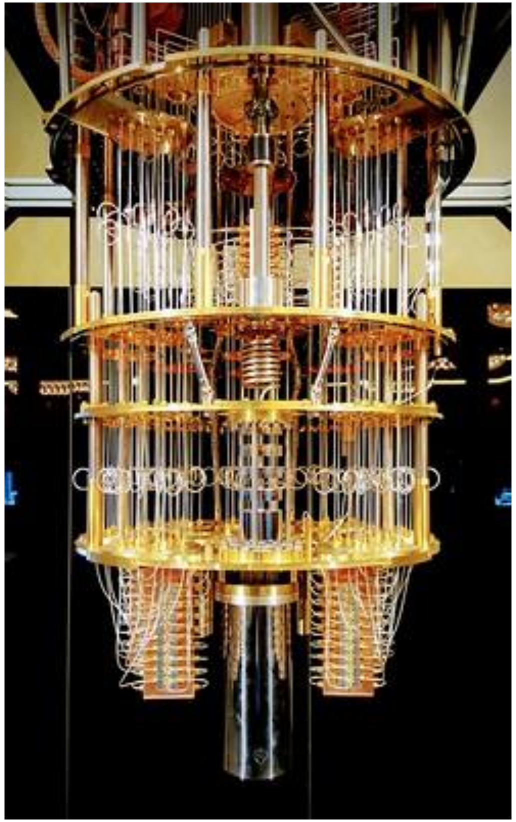


Image source: IBM Q quantum computer

Quantum computers and post-quantum algorithms

A story of Bits and Qubits

Grover's algorithm

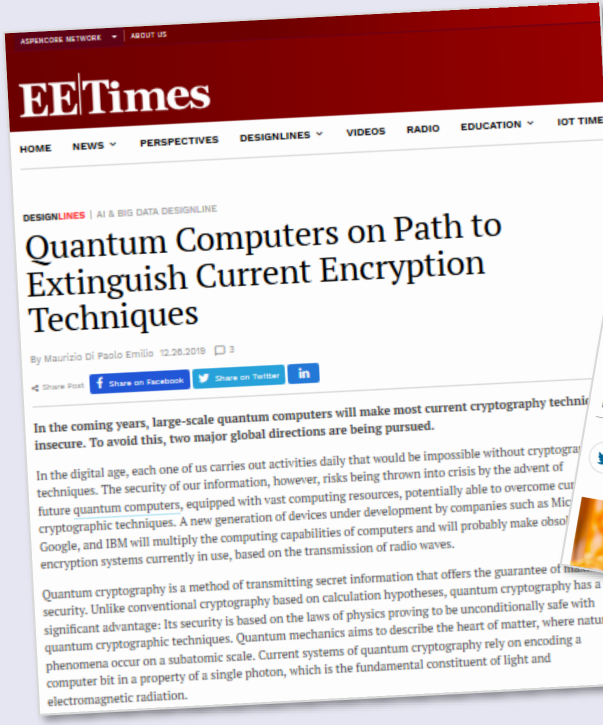
- improves brute-force algorithms that check every possible key. The square-root factor halves the exponent of the time complexity. A brute-force attack on AES-128 with a cost of at most 2^{128} AES-operations on a classical computing system can be finished with about 2^{64} AES-operations on a quantum computer

Shor's algorithm

- solves integer factorization and discrete logs (RSA, ECC) in polynomial time on a quantum computer

Quantum computers and post-quantum algorithms

A story of Bits and Qubits



ASPENCORE NETWORK | ABOUT US

EETimes

HOME NEWS PERSPECTIVES DESIGNLINES VIDEOS RADIO EDUCATION IOT TIME

DESIGNLINES | AI & BIG DATA DESIGNLINE

Quantum Computers on Path to Extinguish Current Encryption Techniques

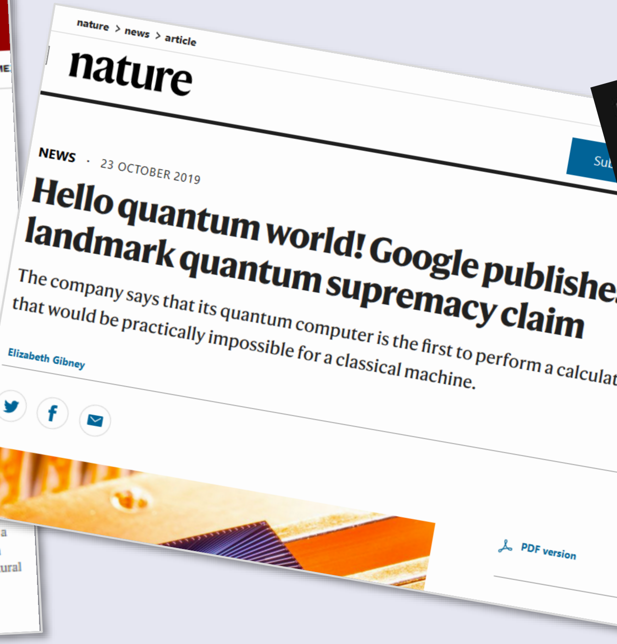
By Maurizio Di Paolo Emilio 12.26.2019 3

Share Post Share on Facebook Share on Twitter in

In the coming years, large-scale quantum computers will make most current cryptography technic insecure. To avoid this, two major global directions are being pursued.

In the digital age, each one of us carries out activities daily that would be impossible without cryptograp techniques. The security of our information, however, risks being thrown into crisis by the advent of future quantum computers, equipped with vast computing resources, potentially able to overcome cur cryptographic techniques. A new generation of devices under development by companies such as Mic Google, and IBM will multiply the computing capabilities of computers and will probably make obsol encryption systems currently in use, based on the transmission of radio waves.

Quantum cryptography is a method of transmitting secret information that offers the guarantee of ma security. Unlike conventional cryptography based on calculation hypotheses, quantum cryptography has a significant advantage: Its security is based on the laws of physics proving to be unconditionally safe with quantum cryptographic techniques. Quantum mechanics aims to describe the heart of matter, where natural phenomena occur on a subatomic scale. Current systems of quantum cryptography rely on encoding a computer bit in a property of a single photon, which is the fundamental constituent of light and electromagnetic radiation.



nature > news > article

nature

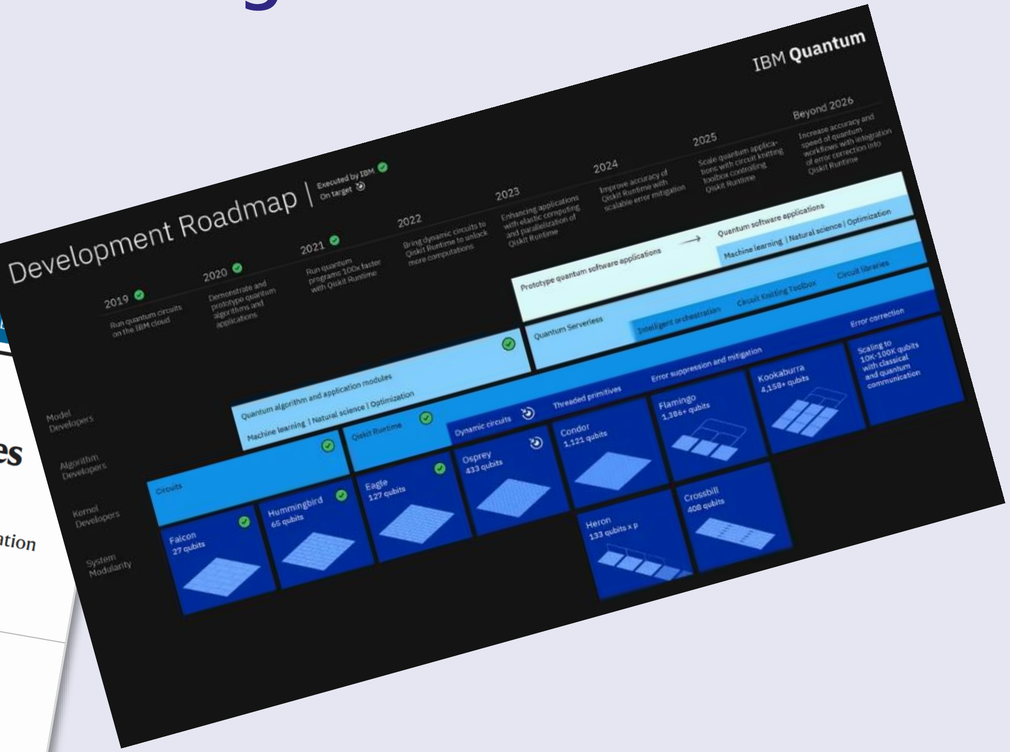
NEWS · 23 OCTOBER 2019

Hello quantum world! Google publishes landmark quantum supremacy claim

The company says that its quantum computer is the first to perform a calculation that would be practically impossible for a classical machine.

Elizabeth Gibney

PDF version



Development Roadmap | Executed by IBM ✓ On target

IBM Quantum

2019 ✓ Run quantum circuits on the IBM cloud

2020 ✓ Demonstrate and prototype quantum algorithms and applications

2021 ✓ Run quantum programs 100x faster with Qiskit Runtime

2022 Bring dynamic circuits to Qiskit Runtime to unlock more computations

2023 Enhancing applications with elastic computing and parallelization of Qiskit Runtime

2024 Improve accuracy of Qiskit Runtime with scalable error mitigation

2025 Scale quantum applications with circuit knitting toolbox controlling Qiskit Runtime

Beyond 2026 Increase accuracy and speed of quantum workflows with integration of error correction into Qiskit Runtime

Model Developers: Quantum algorithm and application modules ✓ Machine learning | Natural science | Optimization; Prototype quantum software applications → Quantum software applications Machine learning | Natural science | Optimization

Algorithm Developers: Qiskit Runtime ✓; Quantum Serverless; Intelligent orchestration; Circuit Knitting Toolbox; Circuit libraries

Kernel Developers: Circuits ✓; Dynamic circuits; Threaded primitives; Error suppression and mitigation; Error correction

System Modularity: Falcon 27 qubits ✓; Hummingbird 65 qubits ✓; Eagle 127 qubits ✓; Osprey 433 qubits; Condor 1,121 qubits; Heron 133 qubits x p; Flamingo 1,386+ qubits; Crossbill 408 qubits; Kookaburra 4,158+ qubits; Scaling to 10K-100K qubits with classical and quantum communication

- https://www.eetimes.com/quantum-computers-on-path-to-extinguish-current-encryption-techniques/
- https://www.nature.com/articles/d41586-019-03213-z
- https://research.ibm.com/blog/ibm-quantum-roadmap-2025

현재까지 구현되어 있는 최대 Qubit 수
- 433 qubit (IBM Osprey)
- 미팅 이후에 더 찾아보니 IBM에서 11월 9일에 새로운 양자 프로세서를 발표 하였습니다. https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two

Quantum computers and post-quantum algorithms

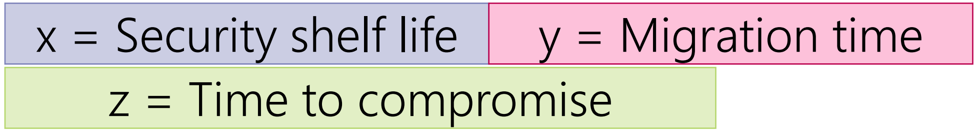
Should we worry?

Public Key cryptography is the most time critical use case!

- Especially public key encryption

The quantum computer threat is a medium-term one but

- Preparation is necessary for products with a long life-cycle
- Several standardization activities are already taking place (e.g. NIST competition, BSI recommendations)



x = Security shelf life

y = Migration time

z = Time to compromise

If x+y > z, then worry!

Michele Mosca: "Cybersecurity in an era with quantum computers: will we be ready?"

Quantum computers and post-quantum algorithms

Post-quantum cryptography

NIST's competition aims at standardizing algorithms for digital signatures and Key encapsulation Mechanisms (KEMs), and is currently in its 4th round.

The post-quantum (PQ) algorithms that are currently in discussion can be divided into five families, according to the different mathematical problems they are based on:

- Hash functions
- Isogenies of elliptic curves
- Lattices
- Linear codes

Status	Public-Key Encryption/KEMs	Digital Signatures
Algorithms to be Standardized	Kyber	Dilithium Falcon SPHINCS+
Algorithms advancing to the 4th Round	BIKE Classic McEliece HQC SIKE	-

Challenges for the automotive industry

Challenges for the automotive industry

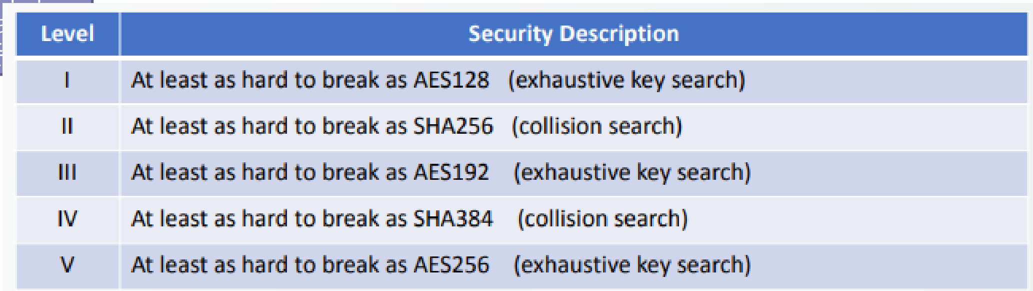
Finding the correct algorithms

Security level의 의미?
암호화 대상마다
사용하는 varia
다른 기준

Finding the most suitable algorithms in the automotive context is a work in progress.

The algorithms need to be compared with respect to:

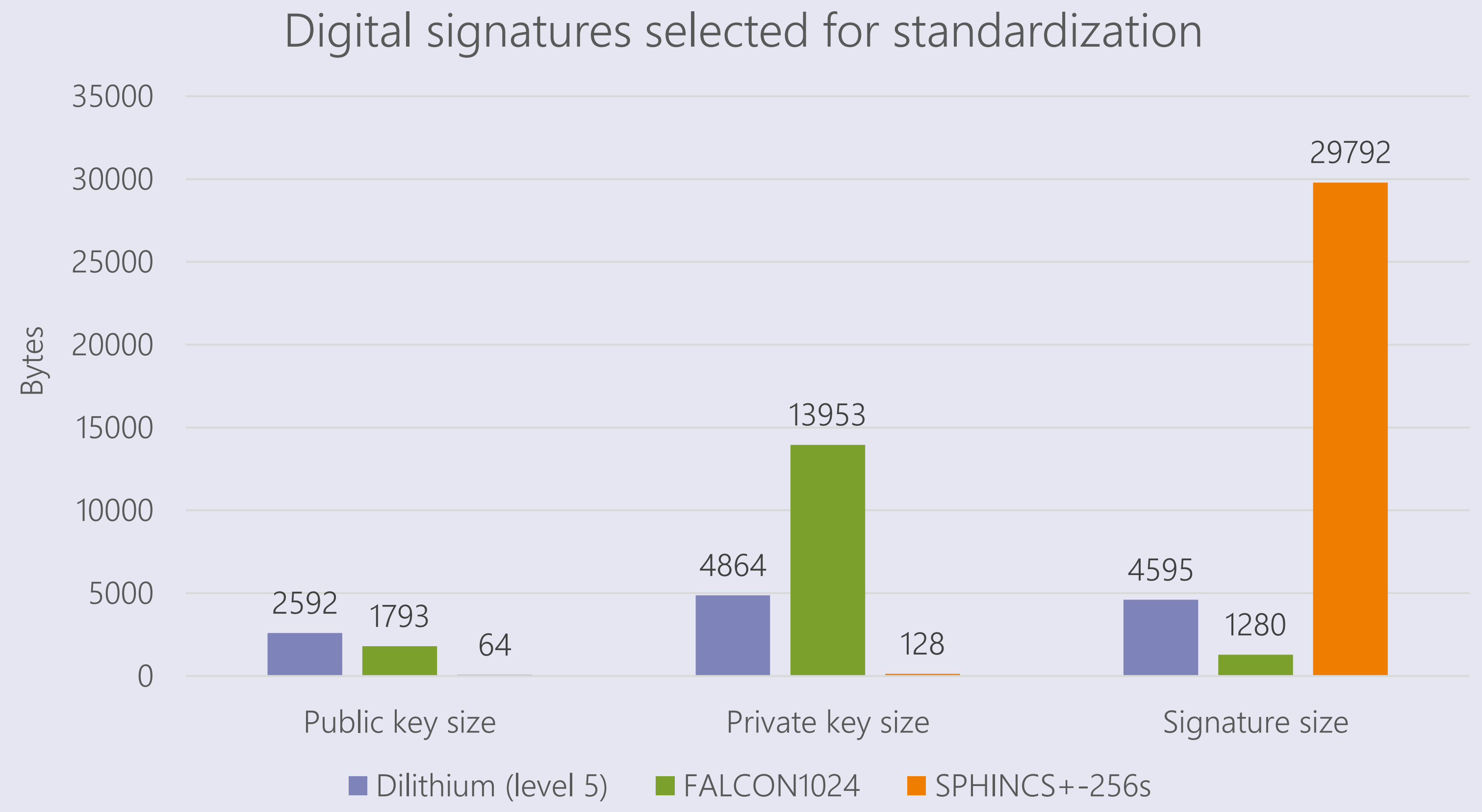
- Secret & public key and signature sizes, code size
- Performance of key generation, signing and verifying algorithms
- Memory consumption during runtime
- Security levels achieved/Confidence in security of algorithms



Level	Security Description
I	At least as hard to break as AES128 (exhaustive key search)
II	At least as hard to break as SHA256 (collision search)
III	At least as hard to break as AES192 (exhaustive key search)
IV	At least as hard to break as SHA384 (collision search)
V	At least as hard to break as AES256 (exhaustive key search)

Challenges for the automotive industry

Finding the correct algorithms

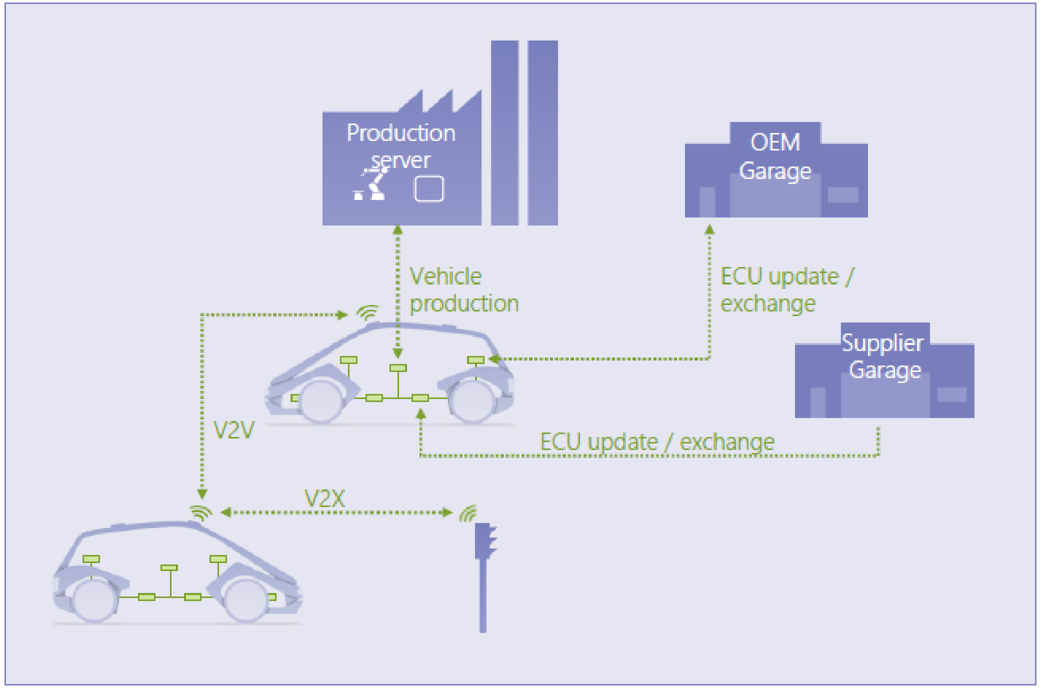


- https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413-upd1.pdf

Challenges for the automotive industry

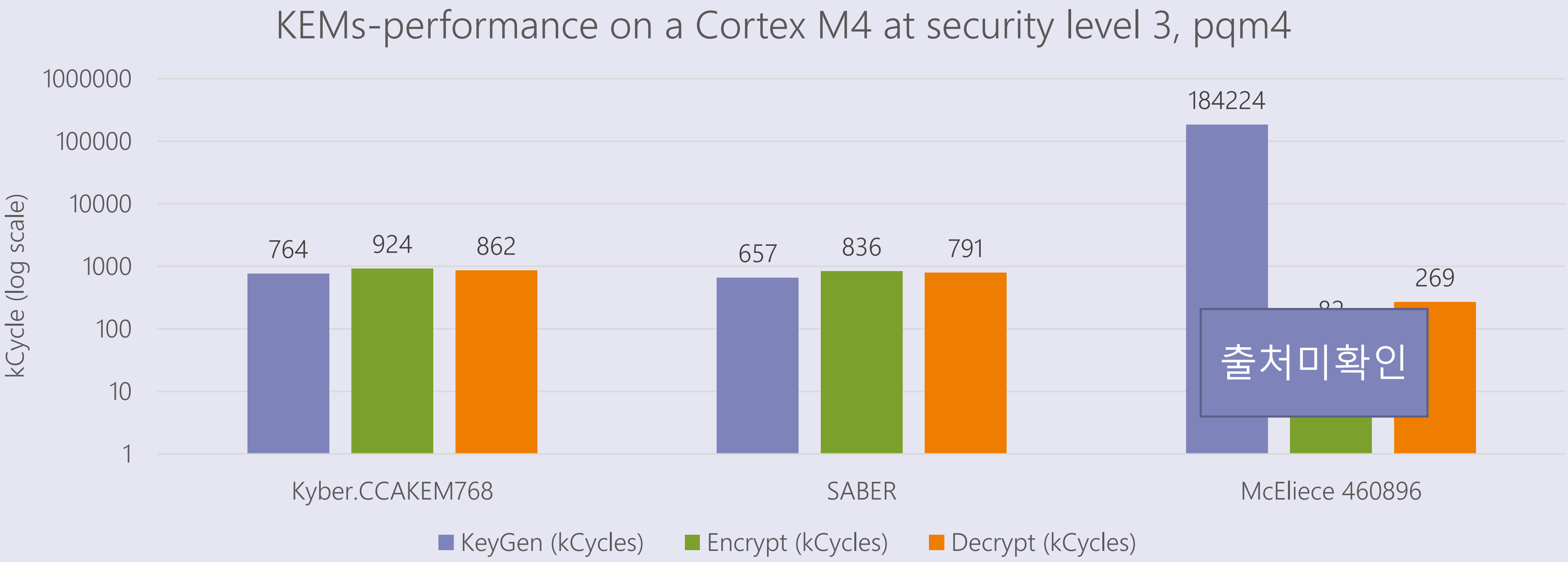
PQ schemes do require more resources –in general-but implementing them in embedded devices, even small ones, is not out of the question

- various benchmarks for embedded devices are available and reference implementations on embedded devices, like a Cortex M4, are widely available



Challenges for the automotive industry

Can PQ-Algorithms even be used in automotive targets?

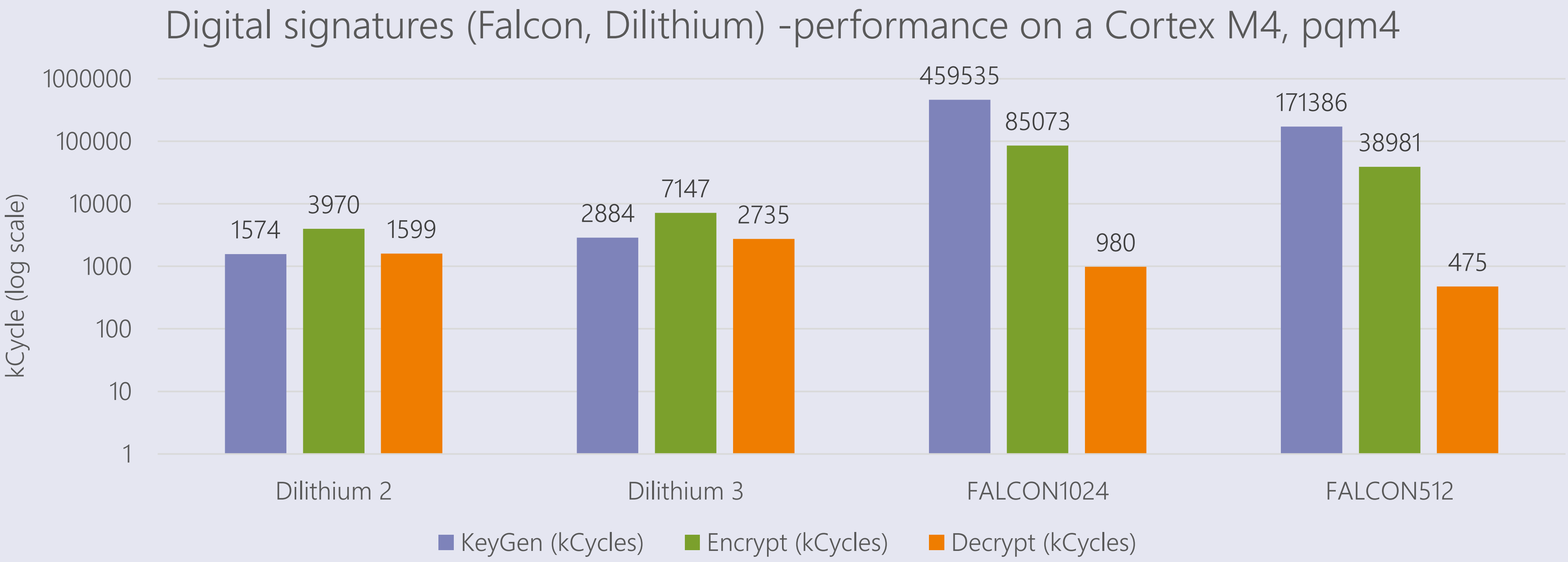


KEMs-performance on a Cortex M4 at security level 3, pqm4

- https://cryptoeng.de/pqdb/comparison

Challenges for the automotive industry

Can PQ-Algorithms even be used in automotive targets?



- https://cryptoeng.de/pqdb/comparison

Challenges for the automotive industry

Finding the correct algorithms… and beyond

OEMs then need to identify:

- which functions/use cases use asymmetric cryptography
  - Different use cases have different requirements, e.g. latency of C2X communication vs latency accepted for communication in production environment
- which use cases are the most time -critical
- which protocols are used and how are they affected by the migration to PQ algorithms

Apart from the selection of the suitable algorithms, many issues need to be considered, such as:

- enabling a smooth transition to quantum-secure systems
- flexible and secure algorithm selection
- adapting the protocols in use
- restructuring the respective PKIs/migrating to new ones
- redesigning of key and certificate management

Challenges for the automotive industry

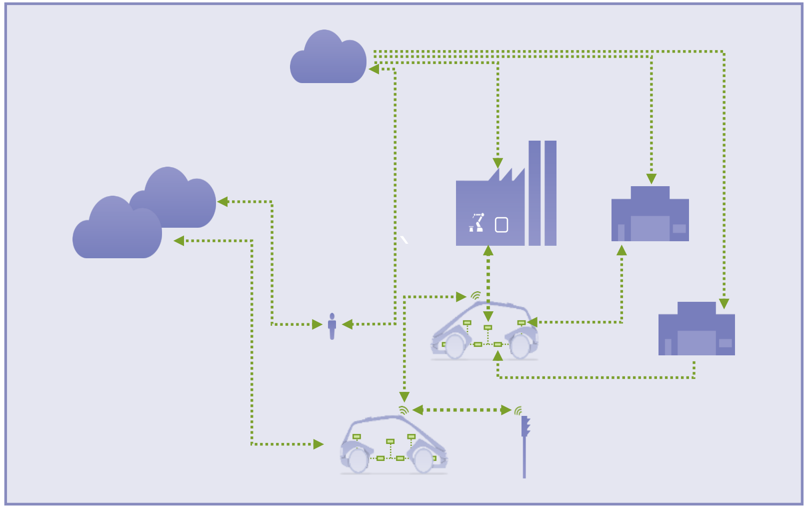
… and possible solutions

Be quantum secure by design:

- Focus on gateways, connectivity ECUs and make them post quantum crypto – enabled
  - These handle the most critical use cases using asymmetric crypto and have less resource constraints
- Use classical certificates to perform updates for ECUs in the field or migrate to another PKI

Important:

- Careful redesigning of the respective PKIs
- Enable migration to a post-quantum PKI, change Root of trust
- Planning for and reserving the necessary resources (RAM/ROM consumption, include hardware security) at an early design phase of the central ECUs

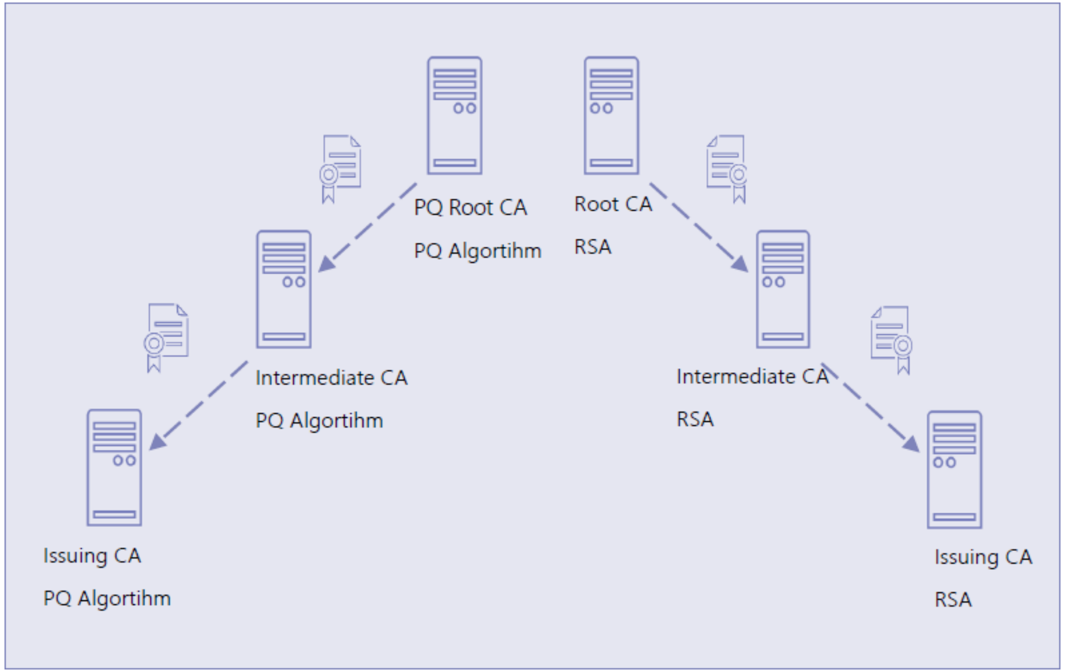


Challenges for the automotive industry

PQ-PKI: Parallel PKI

PKI for ECUs already in the field with no post-quantum upgrade possibilities: parallel PKI

- The OEM PKI could handle this by issuing different certificates in parallel (classical and post-quantum), with only the new ECUs being able to handle the PQ certificates.
- Older ECUs could either use the classical certificates while they are still valid or only get updates in a controlled repair-shop environment, in case the classical certificates are already broken.

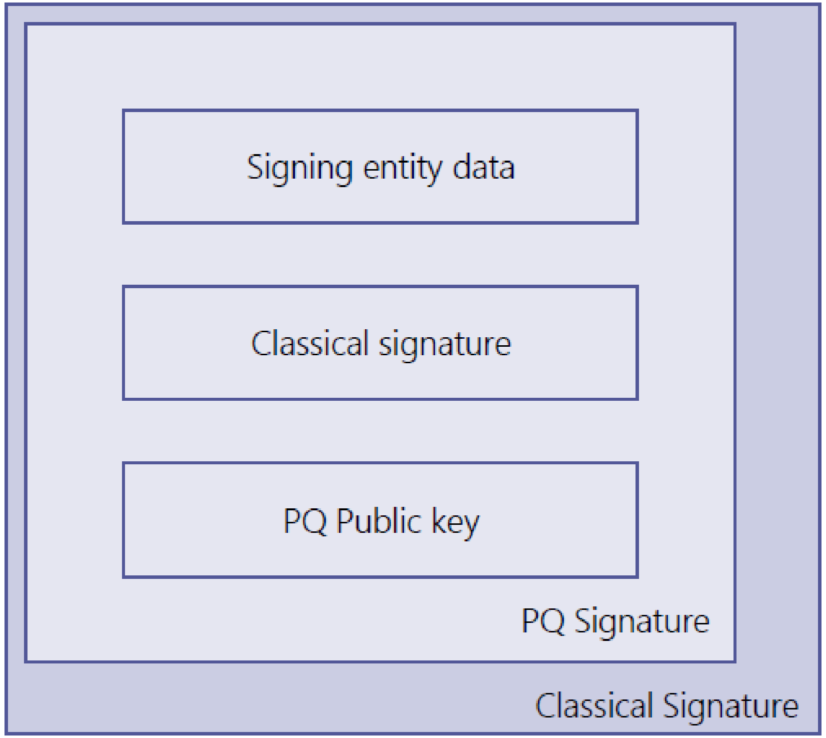


Challenges for the automotive industry

PQ-PKI: Hybrid X.509 certificates

PKI for ECUs already in the field with no post-quantum upgrade possibilities: hybrid PKI

- Certificates contain PQ and classical signature
- If implemented accordingly (e.g. PQ signatures in non-critical extensions of X.509v3 certificates), they offer backwards compatibility
  - An end-entity with no PQ-capabilities can verify only the classical signature
- Used during transition to PQ systems: important to mitigate the risks of downgrade attacks
- Hybrid certificates are already widely studied, different implementations are available

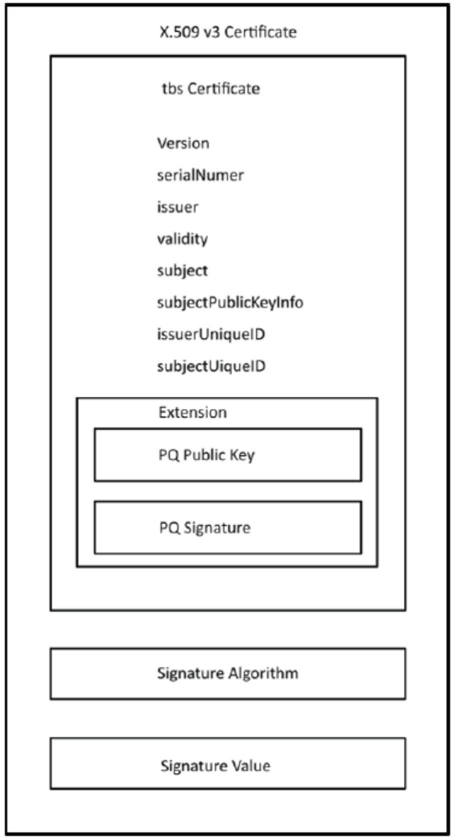


Abstract structure of hybrid certificate

Challenges for the automotive industry

PQ-PKI: Hybrid X.509 certificates

- Implementations of hybrid certificates
  - Open Quantum Safe Project
    - Concatenated keys and signatures inside the certificate
    - no compatibility with non PQ-capable ECUs
  - Nested certificates
    - Include the PQ-signature and the PQ-public key as part of a custom extension.
    - If extension flagged non-critical, then backwards compatible.
    - Outer-certificate non-separable (inner is part of the signed data).

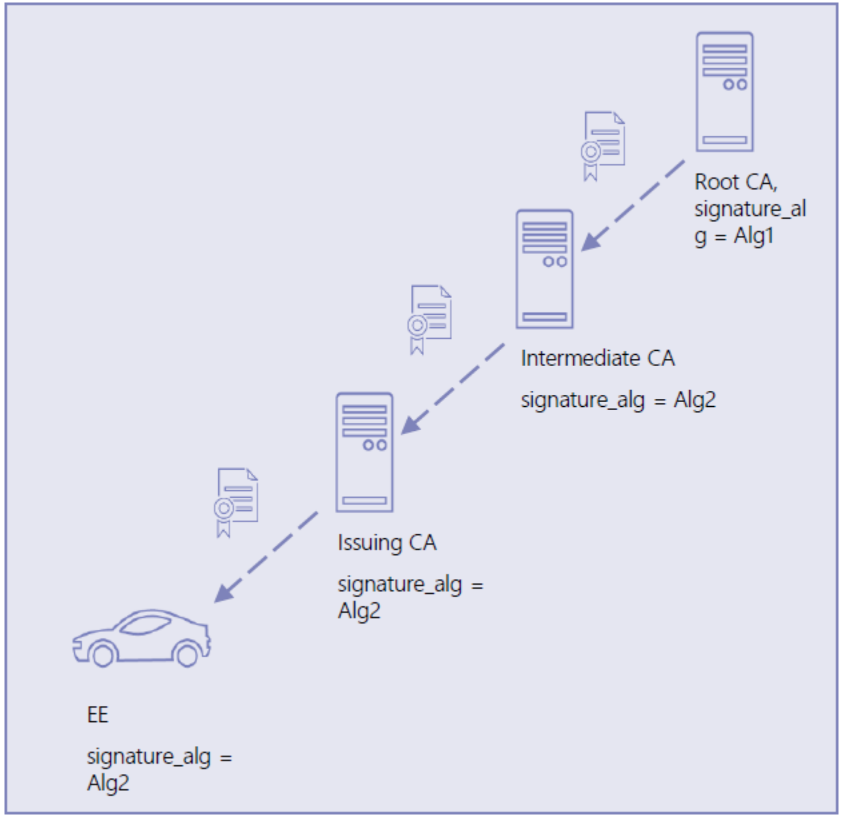


Structure of hybrid certificate-custom extension

Challenges for the automotive industry

Mixed PKI

- Increase security by operating a PKI
  - where the root certificate uses a signing algorithm which is assumed to be more secure (e.g. because of chosen parameter set, or by choosing a well-studied algorithm)
  - end-entities (EE) and intermediate CAs use a different signing algorithm
- Pros:
  - Performance has been shown to be comparable or even better to pure algorithm certificate chains
  - Root of trust offers greater security
  - Requires no changes to X.509 format (compared to hybrid solution)
- Cons:
  - No ad-hoc compatibility non PQ-capable targets
  - Implementation of at least 2 algorithms for signature verification in EE is necessary



Summary

Summary

Post-quantum cryptography in the automotive industry

The transition to quantum-secure systems requires flexible solutions.

- Designing the transition solutions to the post-quantum world is necessary in order to avoid big disruptions
  - For example, hybrid certificates and key exchange can and should be taken into consideration
- Replacing RSA and ECC in the most critical systems takes time and alternative algorithms can already be taken into consideration before NIST’s new standards are finalized

2022.05 KISA
보도자료

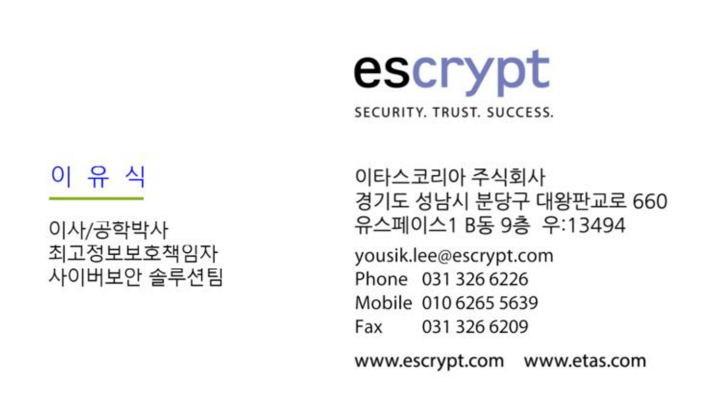
Thank you

ETAS Korea

9F, B, Uspace1,
Daewangpangyo-ro 660,
Bundang-gu, Seongnam-si, Gyeonggi-do,
Rep. of Korea 13494

Phone: +82 31 326 6196
+82 10 9457 0108

Taehyuk.Kim@etas.com
www.escrypt.com



escrypt
SECURITY. TRUST. SUCCESS.

이 유 식

이사/공학박사
최고정보보호책임자
사이버보안 솔루션팀

이타스코리아 주식회사
경기도 성남시 분당구 대왕판교로 660
유스페이스1 B동 9층 우:13494

yousik.lee@escrypt.com
Phone 031 326 6226
Mobile 010 6265 5639
Fax 031 326 6209

www.escrypt.com www.etas.com