secunet

Post-Quantum-Cryptography für Automotive

Makan Rafiee
Team Lead Cryptography & PKI
23.06.2023

Agenda

01 Klassische Kryptographie

02 Quantum Computers

03 Post-Quantum-Cryptography

04 Herausforderungen für Automotive

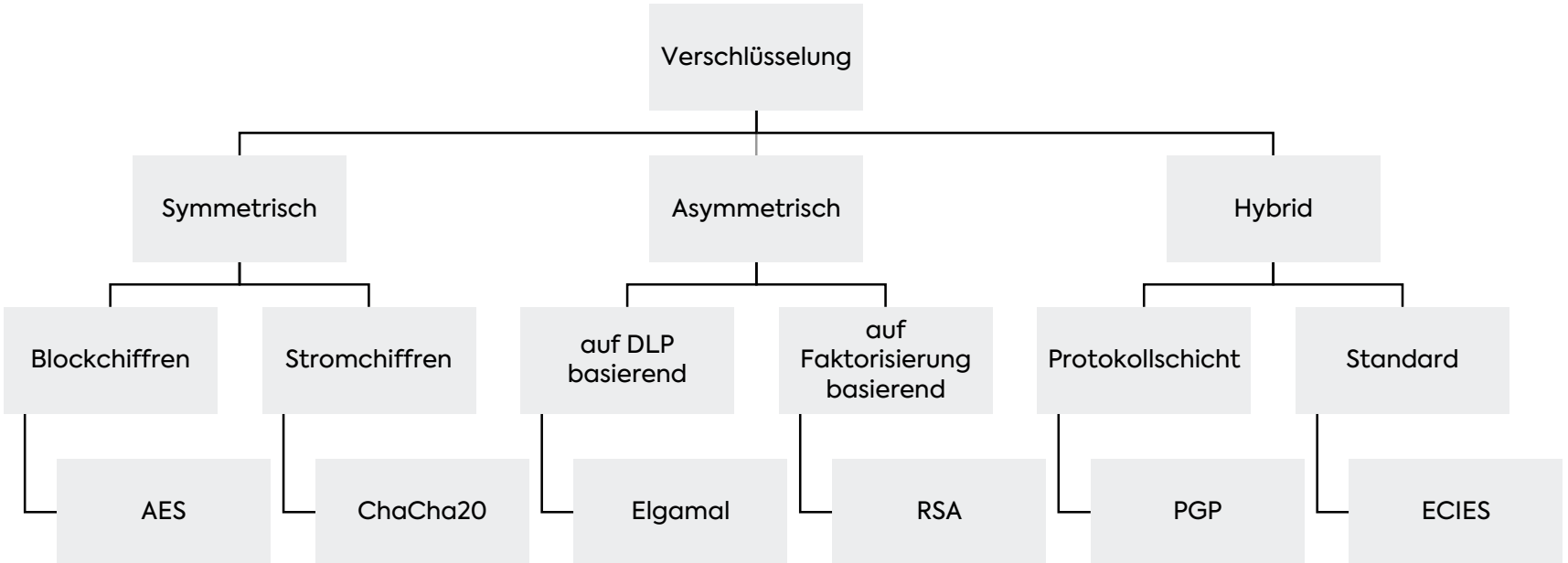
05 Flexible Krypto Agilität

06 Q&A

01

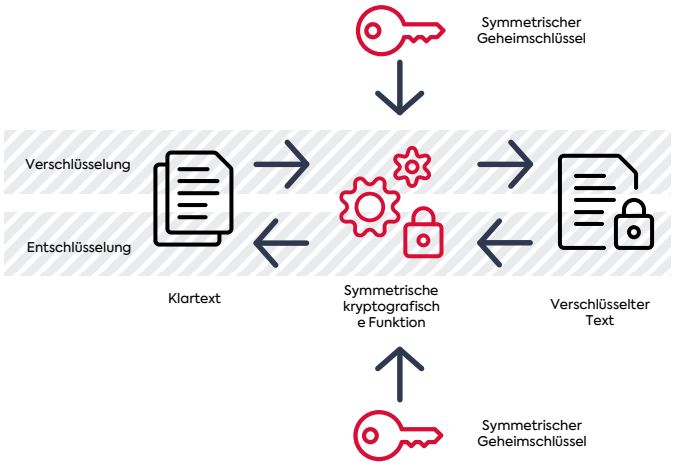
Klassische Kryptographie

Verschiedene Arten von Verschlüsselungsverfahren und Beispiele



Symmetrische Kryptographie

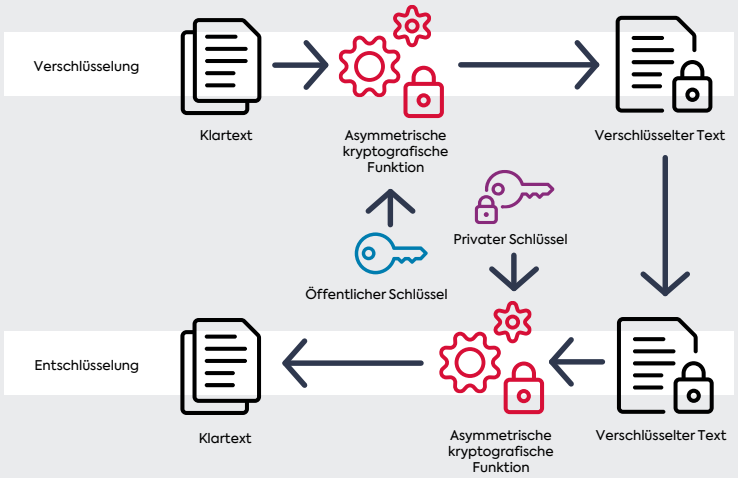
- Verfahren basieren meist auf effizienten Operationen wie Bit-Shifts und XORs
- Ver- und Entschlüsselung sehr schnell
- Schlüsselraum = ganzer Zahlenraum



vs.

Asymmetrische Kryptographie

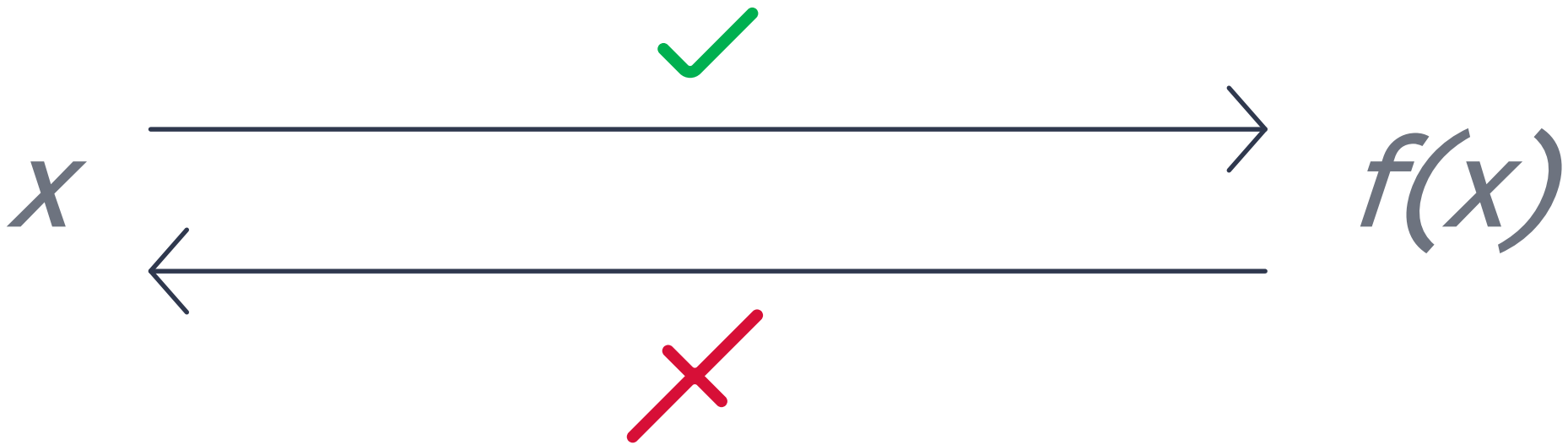
- Basiert auf mathematischen Einwegfunktionen.
- Ver- und Entschlüsselung sehr langsam.
- Verschlüsselung nur möglich für kleine Daten (kleiner als den Zahlenraum)



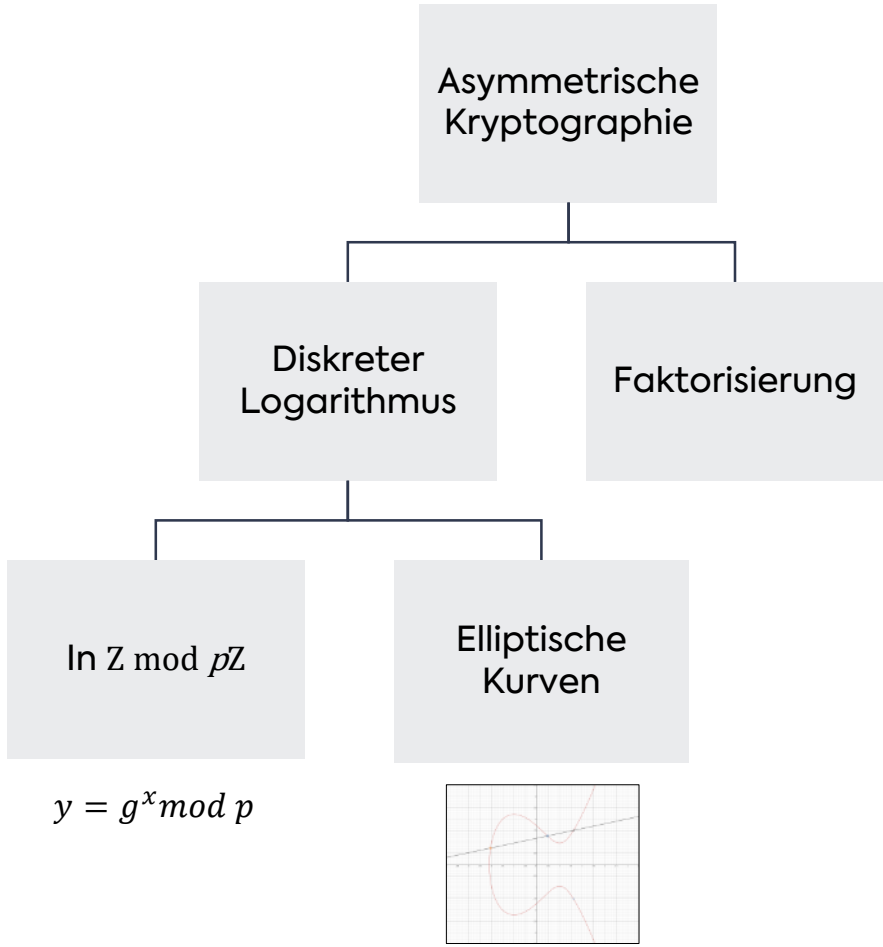
Kombinieren beider Verfahren ➔ hybride Verschlüsselung (z.B. ECIES, PGP)

Einwegfunktionen

Eine Einwegfunktion ist eine mathematische Funktion, die
- „leicht“ berechenbar
- aber „schwer“ umzukehren ist.



Einwegfunktionen in klassischer Kryptographie

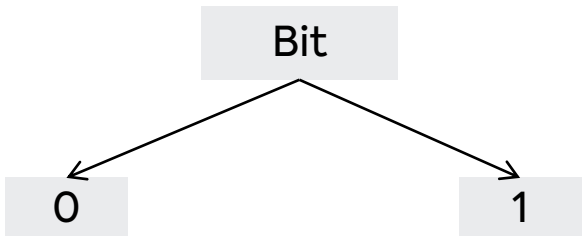


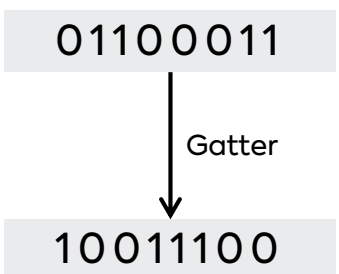
02

Quantum Computers

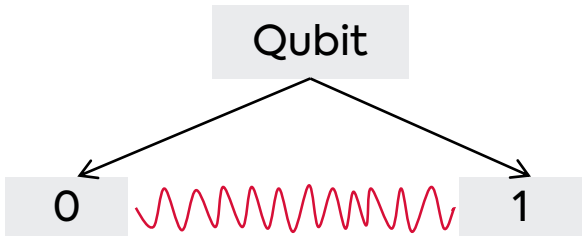
Grundlagen Quantencomputer

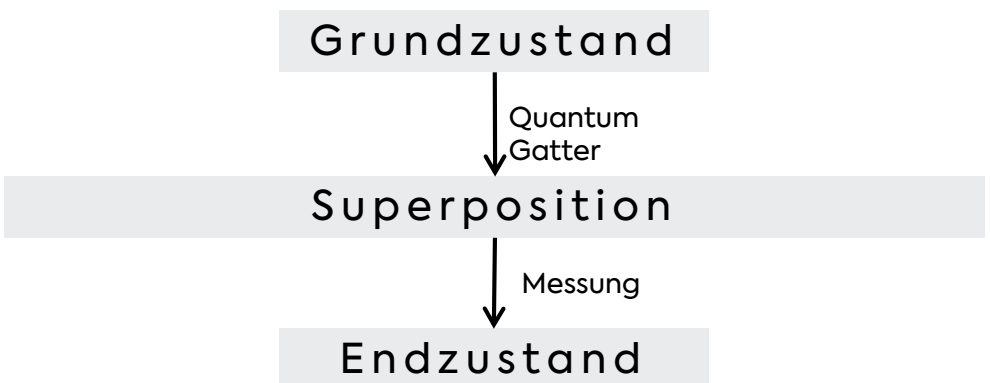
Klassischer Computer



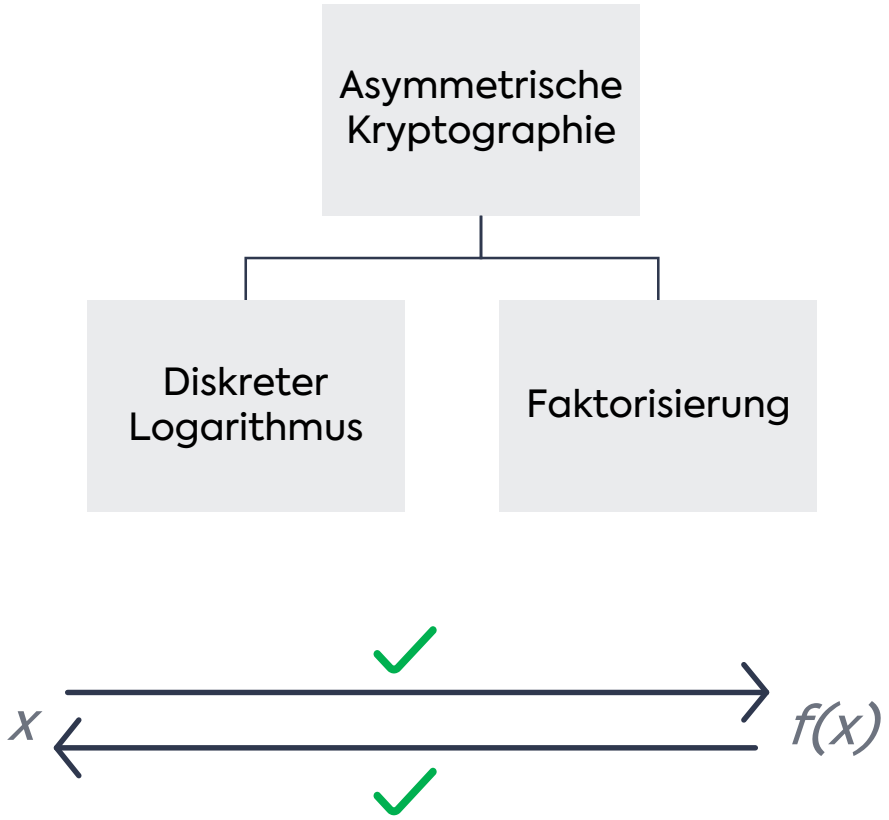


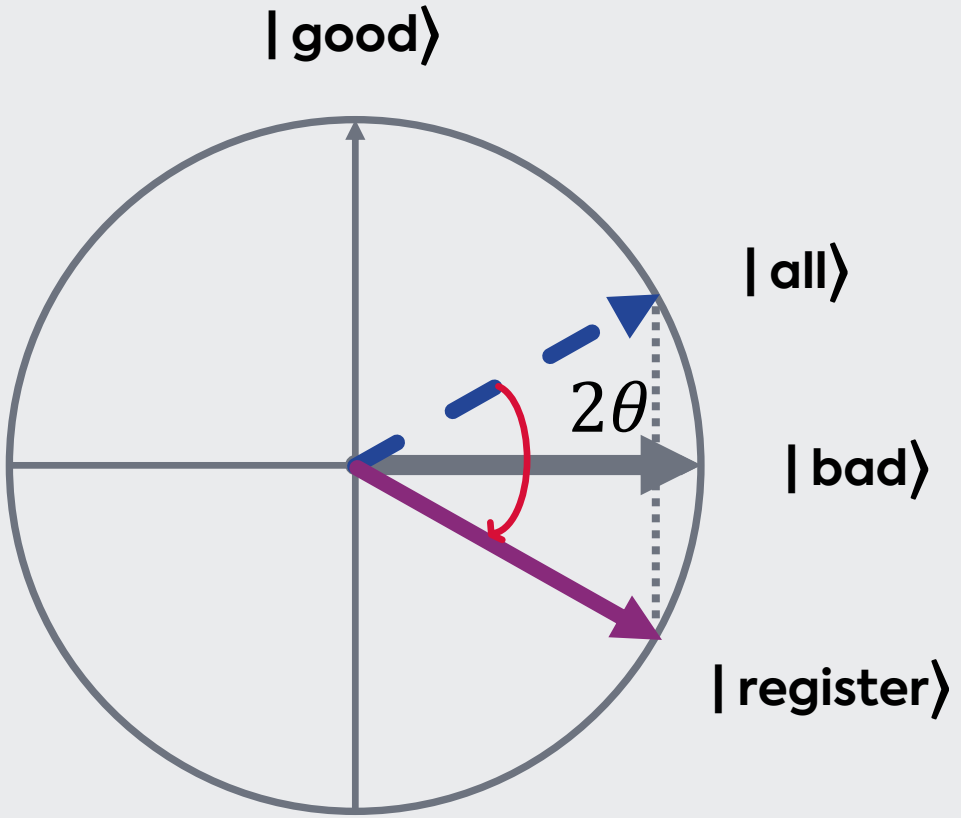
Quantencomputer





SHOR-Algorithmus vs. GROVER-Algorithmus





Applying O_f

Konventionelle Algorithmen

*In cryptography, **security level** is a measure of the strength that a cryptographic primitive — such as a cipher or hash function — achieves. Security level is usually expressed in "bits", where n-bit security means that the attacker would have to perform 2^n operations to break it.*

Algorithmus	Schlüssellange	Sicherheitsniveau (Klassisch)	Sicherheitsniveau (Quantum)
RSA-3072	3072 Bit	128 Bit	35 Bit
RSA-7680	7680 Bit	192 Bit	38 Bit
RSA-15360	15360 Bit	256 Bit	41 Bit
ECC-256	256 Bit	128 Bit	35 Bit
AES-128	128 Bit	128 Bit	64 Bit
AES-256	256 Bit	256 Bit	128 Bit

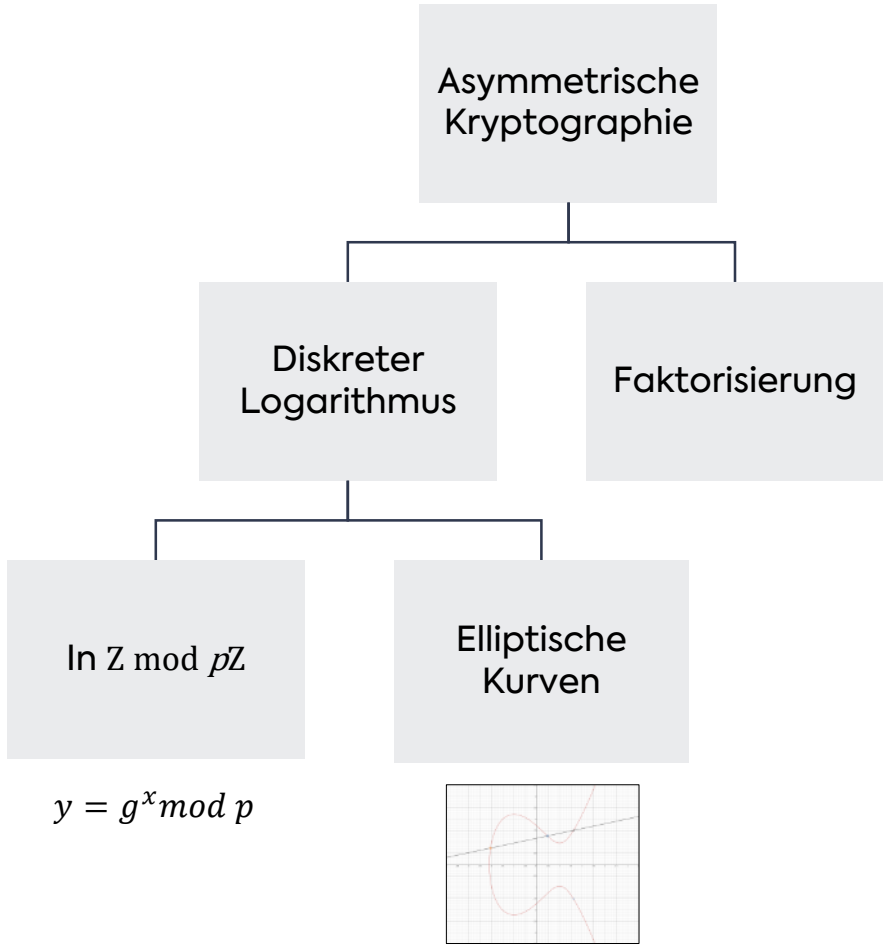
Shor-Algorithmus

Grover-Algorithmus

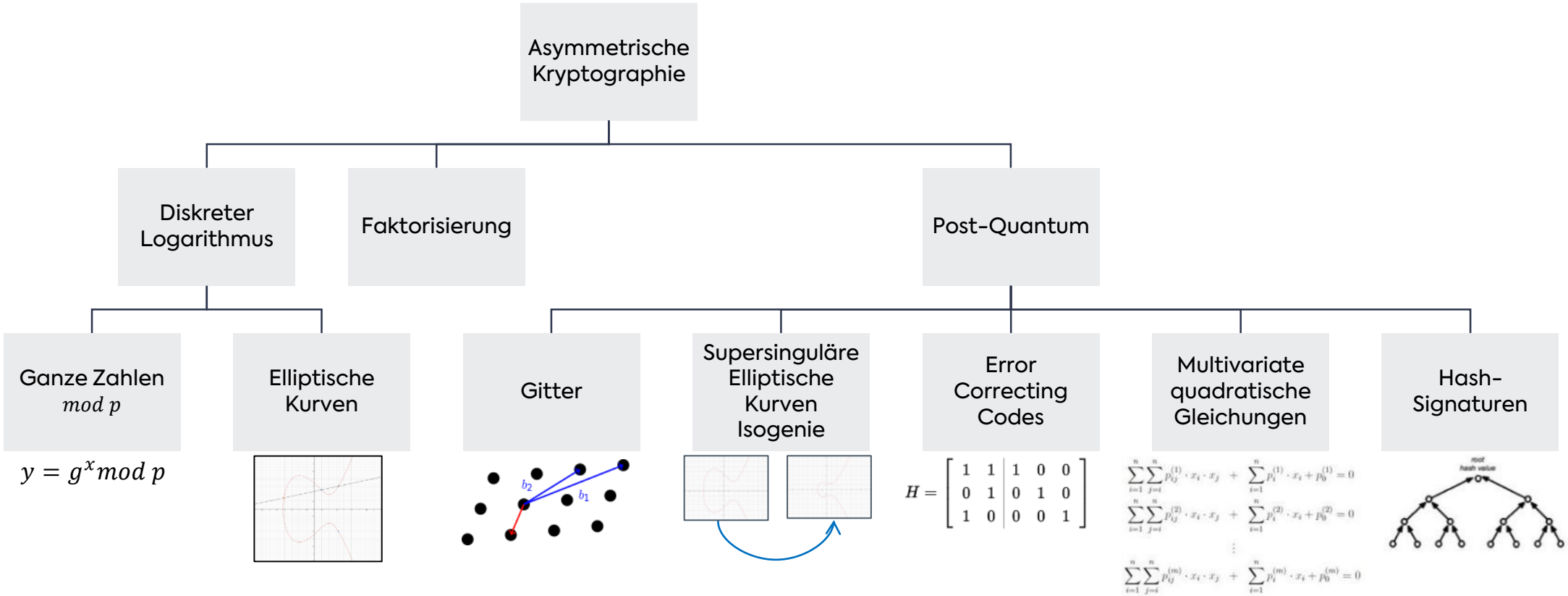
03

Post-Quantum Cryptography

Einwegfunktionen für klassische Kryptographie



Einwegfunktionen für Post-Quantum Kryptographie



Runde 1

Type	PKE/KEM	Signature
Lattice	**Compact LWE, CRYSTALS-Kyber, Ding Key Exchange, EMBLEM and R.EMBLEM, FrodoKEM, ~~HILA5~~ *(withdrawn and merged into Round5)*, KCL (pka OKCN/AKCN/CNKE), KINDI, LAC, LIMA, Lizard, LOTUS, NewHope, NTRUEncrypt, NTRU-HRSS-KEM, NTRU Prime, Odd Manhattan, ~~Round2~~ *(withdrawn and merged into Round5)*, Round5 *(merger of Round2 and Hila5)*,SABER, Three Bears, Titanium**	**CRYSTALS-Dilithium, DRS, FALCON, pqNTRUSign, qTESLA**
Code	**BIG QUAKE, BIKE, Classic McEliece + NTS-KEM, DAGS, ~~Edon-K,~~ HQC, ~~LAKE~~ *(withdrawn and merged into ROLLO)*, LEDAkem, LEDApkc, Lepton, ~~LOCKER~~ *(withdrawn and merged into ROLLO)*, McNie, NTS-KEM, ROLLO *(merger of Ouroboros-R, LAKE and LOCKER)*, ~~Ouroboros-R~~ *(withdrawn and merged into ROLLO)*, QC-MDPC KEM, Ramstake, RLCE-KEM, RQC**	**pqsigRM, RaCoSS, ~~RankSign~~**
Hash		**Gravity-SPHINCS, SPHINCS+**
Supersingular Isogeny	**SIKE**	
Multivariate	**CFPKM, Giophantus**	**DualModeMS, GeMSS, Gui, HiMQ-3, LUOV, MQDSS, Rainbow**

Runde 2

Type	PKE/KEM	Signature
Lattice	Compact LWE, **CRYSTALS-Kyber**, Ding Key Exchange, EMBLEM and R.EMBLEM, **FrodoKEM**, ~~HILA5~~ *(withdrawn and merged into Round5)*, KCL (pka OKCN/AKCN/CNKE), KINDI, **LAC**, LIMA, Lizard, LOTUS, **NewHope**, **NTRUEncrypt, NTRU-HRSS-KEM**, **NTRU Prime**, Odd Manhattan, ~~Round2~~ *(withdrawn and merged into Round5)*, **Round5** ***(merger of Round2 and Hila5)***,**SABER**, **Three Bears**, Titanium	**CRYSTALS-Dilithium**, DRS, **FALCON**, pqNTRUSign, **qTESLA**
Code	BIG QUAKE, **BIKE**, **Classic McEliece** + NTS-KEM, DAGS, ~~Edon-K,~~ **HQC**, ~~LAKE~~ *(withdrawn and merged into ROLLO)*, **LEDAkem, LEDApkc**, Lepton, ~~LOCKER~~ *(withdrawn and merged into ROLLO)*, McNie, **NTS-KEM**, **ROLLO** ***(merger of Ouroboros-R, LAKE and LOCKER)***, ~~Ouroboros-R~~ *(withdrawn and merged into ROLLO)*, QC-MDPC KEM, Ramstake, RLCE-KEM, **RQC**	pqsigRM, RaCoSS, ~~RankSign~~
Hash		Gravity-SPHINCS, **SPHINCS+**
Supersingular Isogeny	**SIKE**	
Multivariate	CFPKM, Giophantus	DualModeMS, GeMSS, Gui, HiMQ-3, LUOV, MQDSS, Rainbow

Runde 3 (+ Alternativen)

Type	PKE/KEM	Signature
Lattice	Compact LWE, **CRYSTALS-Kyber**, Ding Key Exchange, EMBLEM and R.EMBLEM, **FrodoKEM**, ~~HILA5~~ *(withdrawn and merged into Round5)*, KCL (pka OKCN/AKCN/CNKE), KINDI, LAC, LIMA, Lizard, LOTUS, NewHope, **NTRU**, **NTRU Prime**, Odd Manhattan, ~~Round2~~ *(withdrawn and merged into Round5)*, Round5 *(merger of Round2 and Hila5)*,**SABER**, Three Bears, Titanium	**CRYSTALS-Dilithium**, DRS, **FALCON**, pqNTRUSign, qTESLA
Code	BIG QUAKE, **BIKE**, **Classic McEliece** + NTS-KEM, DAGS, ~~Edon-K,~~ **HQC**, ~~LAKE~~ *(withdrawn and merged into ROLLO)*, LEDAkem, LEDApkc, Lepton, ~~LOCKER~~ *(withdrawn and merged into ROLLO)*, McNie, NTS-KEM, ROLLO *(merger of Ouroboros-R, LAKE and LOCKER)*, ~~Ouroboros-R~~ *(withdrawn and merged into ROLLO)*, QC-MDPC KEM, Ramstake, RLCE-KEM, RQC	pqsigRM, RaCoSS, ~~RankSign~~
Hash		Gravity-SPHINCS, **SPHINCS+**
Supersingular Isogeny	**SIKE**	
Multivariate	CFPKM, Giophantus	DualModeMS, **GeMSS**, Gui, HiMQ-3, LUOV, MQDSS, Rainbow

Gewinner

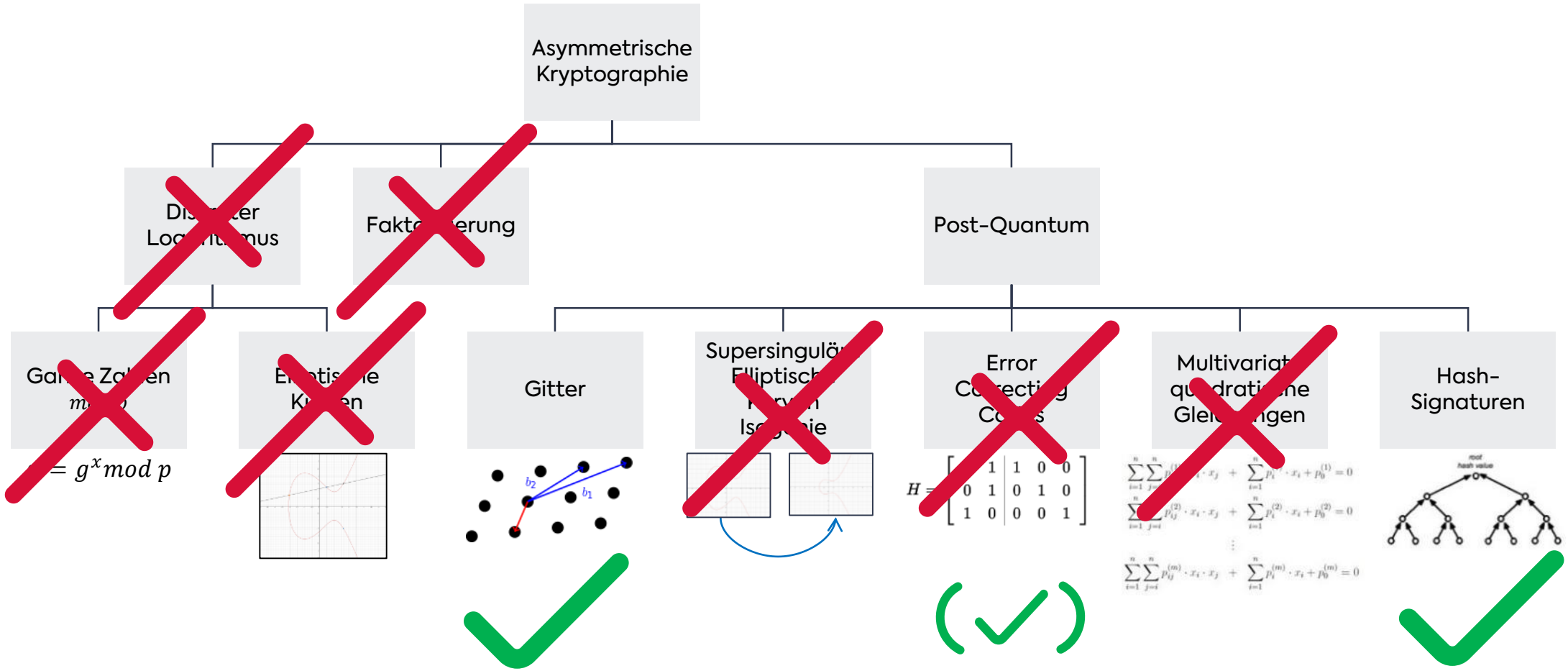
Type	PKE/KEM	Signature
Lattice	**CRYSTALS-Kyber**	**CRYSTALS-Dilithium** **FALCON**
Code		
Hash		**SPHINCS+**
Supersingular Isogeny		
Multivariate		

Runde 4

Type	PKE/KEM	Signature
Lattice		
Code	**BIKE** **Classic McEliece** **HQC**	
Hash		
Supersingular Isogeny	**SIKE (BROKEN 5. AUGUST)**	
Multivariate		

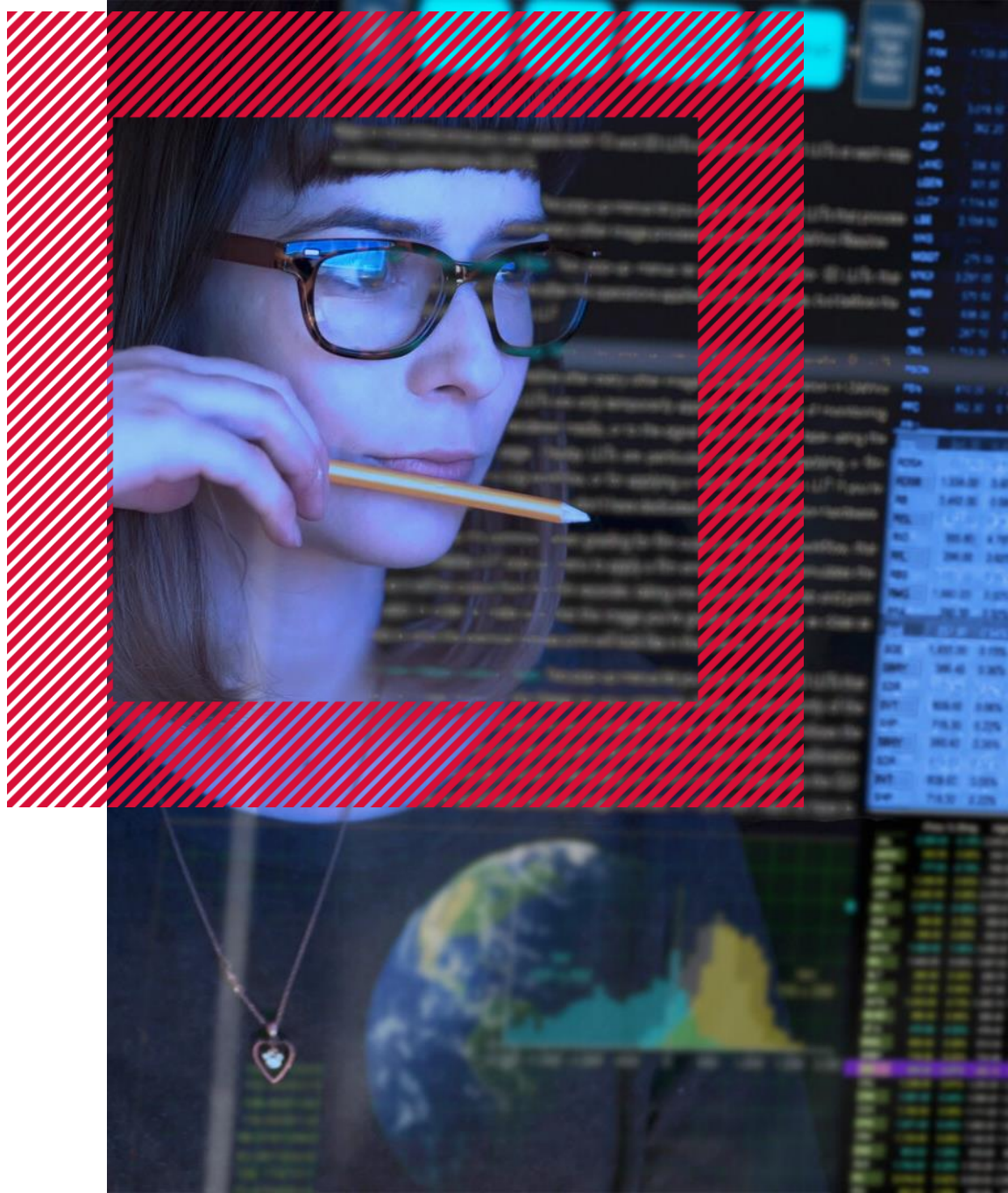
*"**Four additional algorithms are under consideration** for inclusion in the standard, and NIST plans to announce the finalists from that round at a future date. NIST is announcing its choices in two stages **because of the need for a robust variety of defense tools**. As cryptographers have recognized from the beginning of NIST's effort, there are different systems and tasks that use encryption, and a useful standard would **offer solutions designed for different situations, use varied approaches for encryption, and offer more than one algorithm** for each use case in the event one proves vulnerable." [1]*

Überblick Asymmetrische Kryptografie



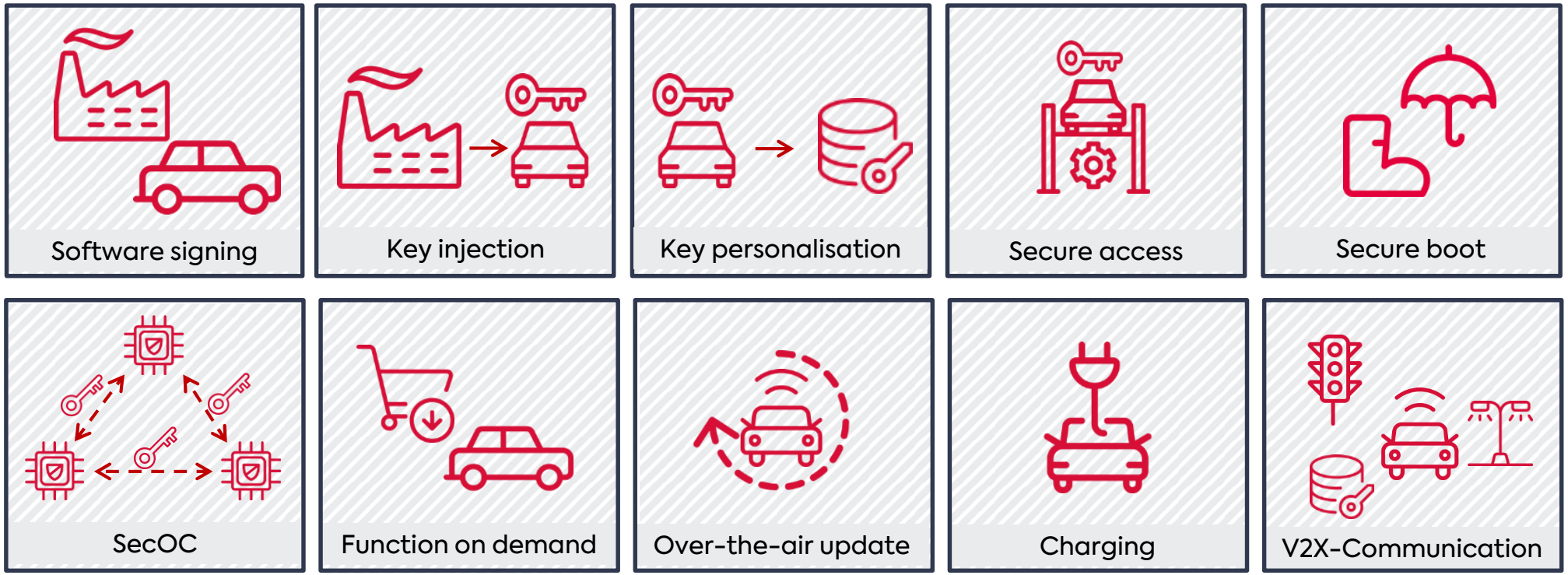
04

Herausforderungen für Automotive



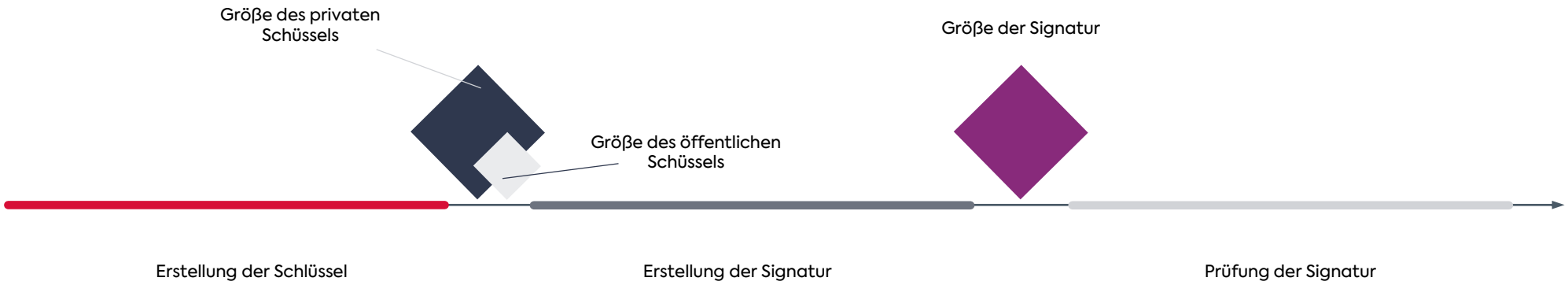
Herausforderungen für Automotive

Encryption | **Key Agreement** | **Digital Signature**



05

Flexible Krypto Agilität


Größe des privaten Schüssels
Größe des öffentlichen Schüssels
Größe der Signatur
Erstellung der Schlüssel
Erstellung der Signatur
Prüfung der Signatur

Post-Quantum-Algorithmen

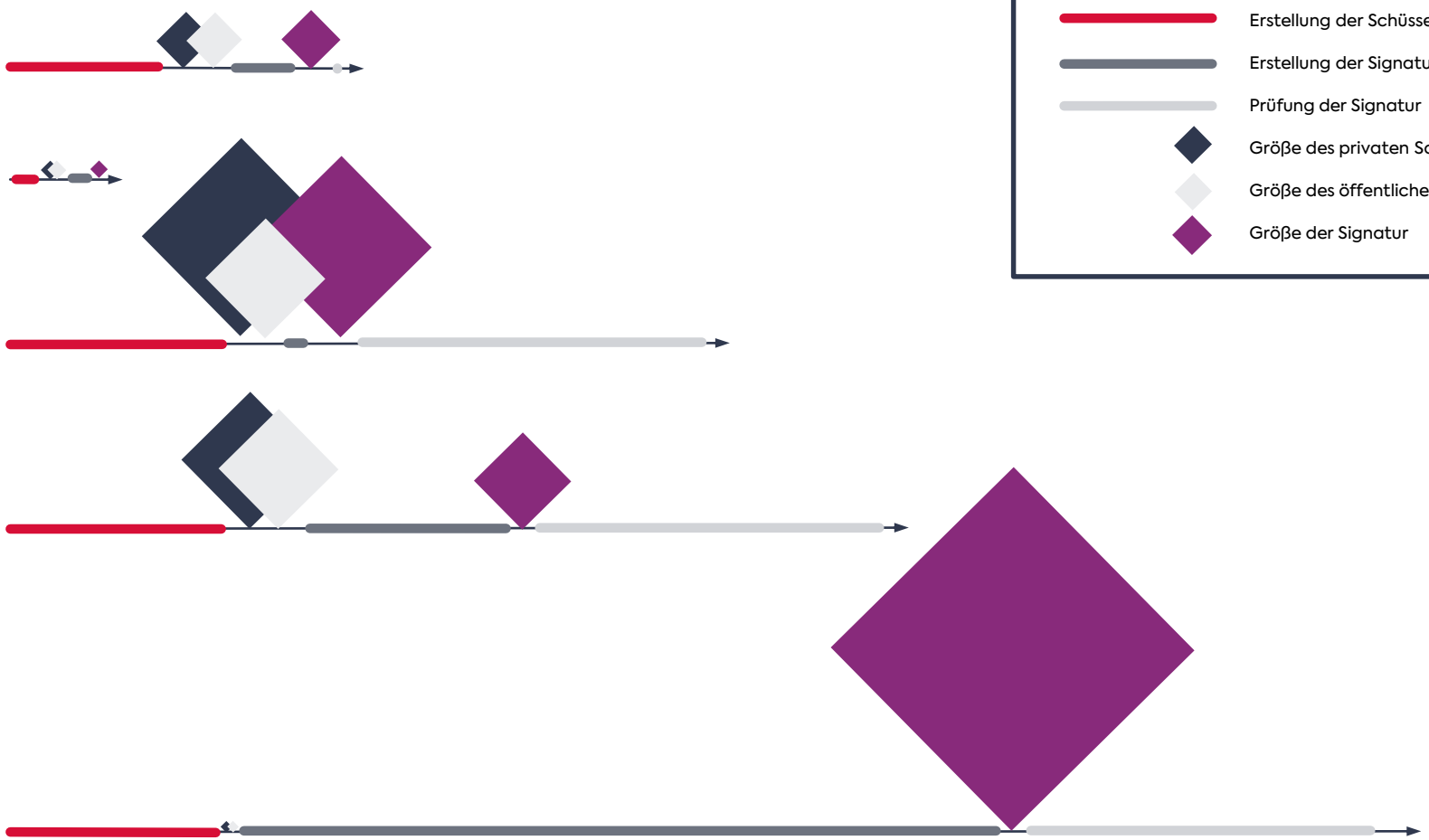
RSA-3072

ECDSA-384

Dilithium IV

FALCON 1024

SPHINX+ 256



06

Q&A


secunet