SECURWARE 2024

THEORETICAL AND PRACTICAL ASPECTS IN IDENTIFYING GAPS AND PREPARING FOR POST-QUANTUM CRYPTOGRAPHY

Jörn-Marc Schmidt and Alexander Lawall
IU International University of Applied Science
Erfurt, Thüringen, Germany

SPEAKER

Jörn-Marc Schmidt

joern-marc.schmidt@iu.org

- Since 2024: *Professor Cybersecurity*
  IU Internationale Hochschule
- 2018–2023 *Lead Engineer*, Cryptography Engineering and Solutions,
  Deutsche Bank AG, Eschborn, Germany
- 2013–2018 *Senior IT-Security Consultant*, secunet Security Networks AG,
  Eschborn, Germany
- 2010–2013 *Group coordinator,* Institute for Applied Information Processing and
  Communication (IAIK), Technischen Universität Graz, Austria
- 2006–2009 Ph.D. Studies at Graz University of Technology, Graz, Austria
- 2002–2006 Study at University of Mannheim, Mannheim, Germany

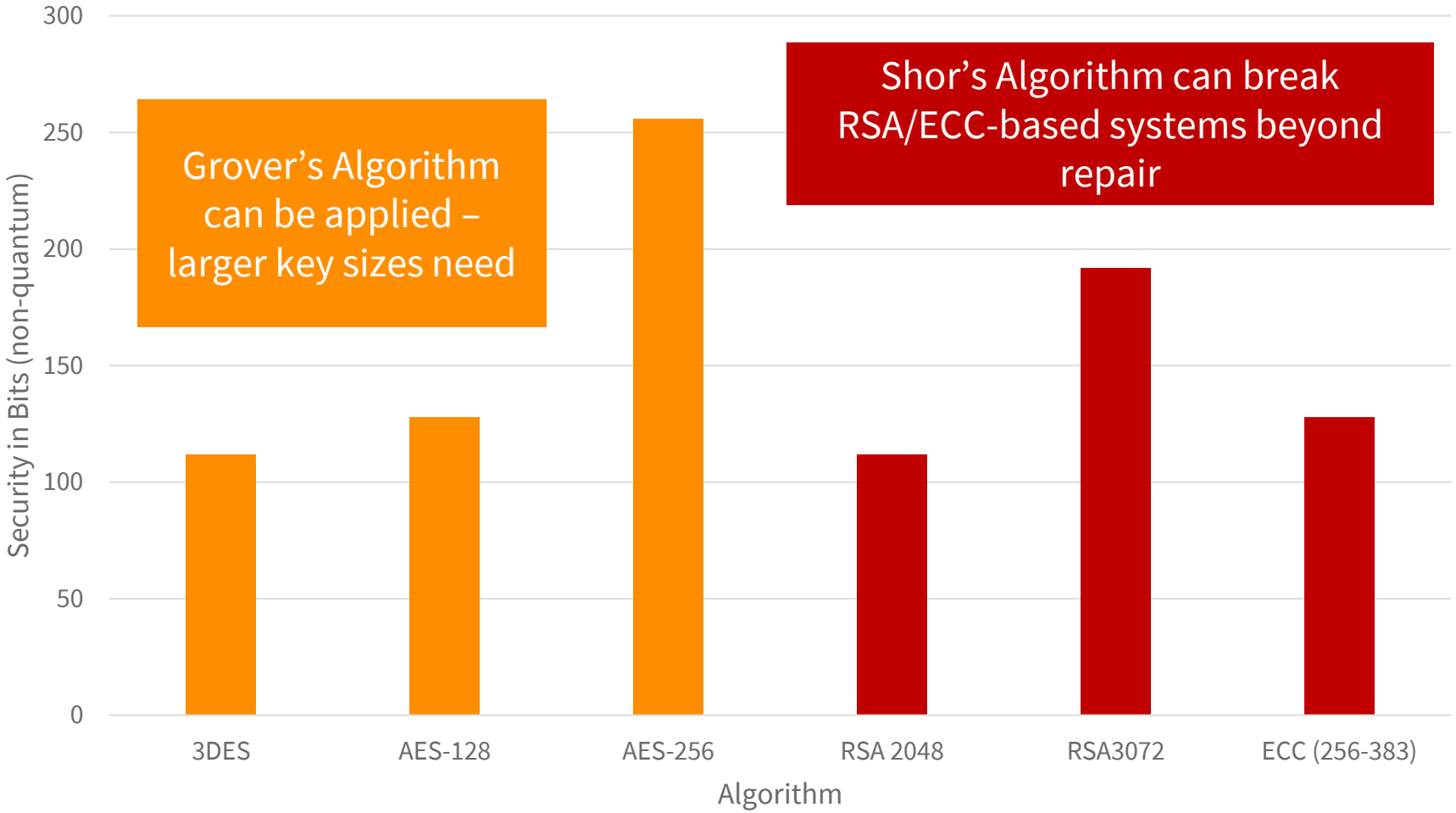
AGENDA

QUANTUM COMPUTERS

- Rely on quantum effects like
  - superposition and entanglement
- Use qubits
- Provide non-deterministic results

- Can solve specific problems faster, like
  - Biological and chemical simulations
  - Risk modeling
  - Solving optimization problems

IMPACT ON CRYPTOGRAPHY

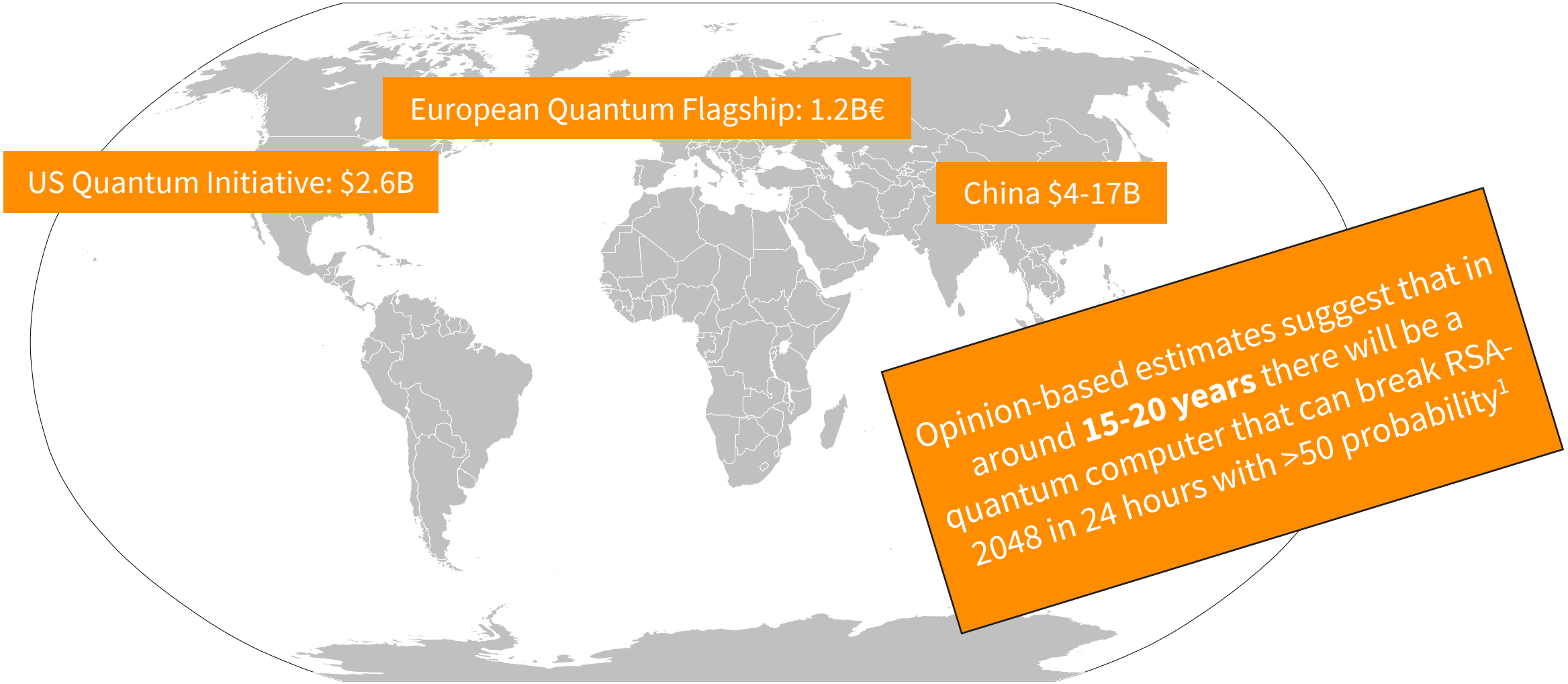


Grover's Algorithm can be applied – larger key sizes need

Shor's Algorithm can break RSA/ECC-based systems beyond repair

Currently, no quantum computer that endangers common algorithms / key sized exists.

QUANTUM COMPUTERS -INVESTMENTS



Global investments reached $42B Dollars in 2023

Image by Canuckguy et al., Public domain, via Wikimedia Commons

[1] Discussed in „The Quantum Threat Timeline Report 2023" by Dr. Michele Mosca and Dr. Marco Piani

SO, WHY WORRY TODAY?

INTERNATIONAL UNIVERSITY OF APPLIED SCIENCES

Moscas Theorem

Mitigation Time + Data Lifetime

Time till a Quantum Computer can decrypt your data

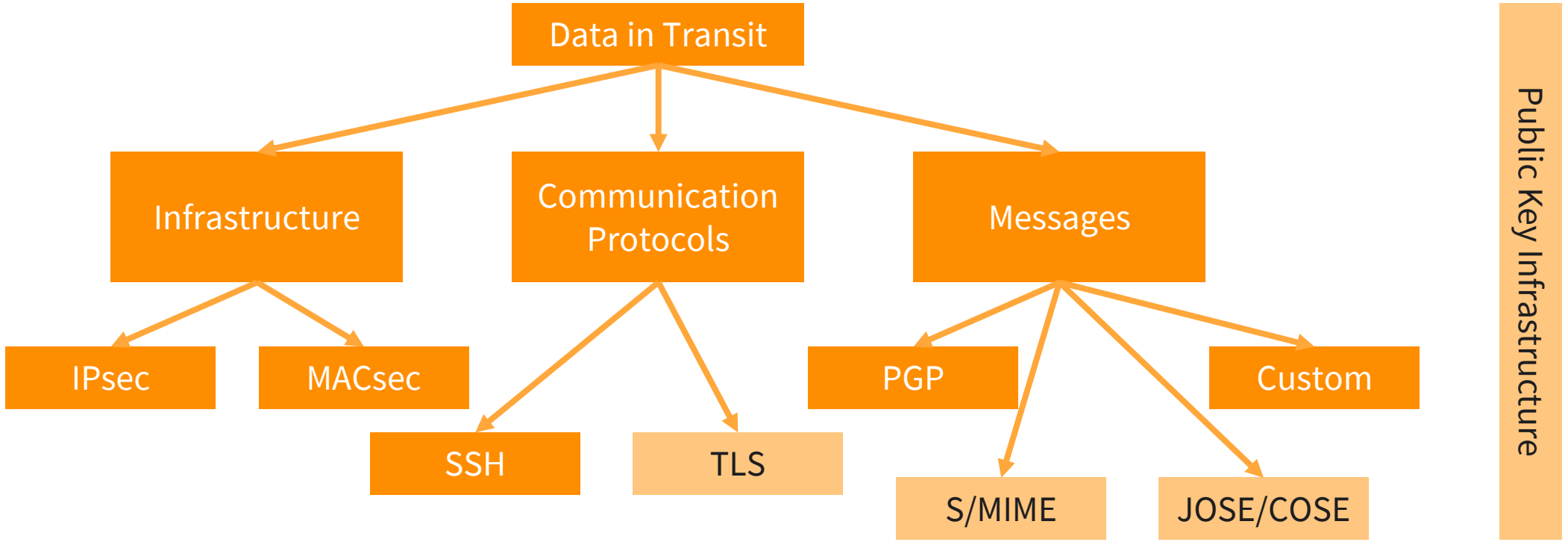
} Consider your mitigation & how long your data needs to stay confidential

Harvest and Decrypt Attack

- Record transmitted data now
- Decrypt them when quantum computers are available

→ Issue for data that require long-term confidentiality

WHERE TO START?



Post-Quantum Cryptography (PQC) required as basis to replace asymmetric algorithms

Post-Quantum Cryptography (PQC) required as basis to replace asymmetric algorithms

INTERNATIONAL UNIVERSITY OF APPLIED SCIENCES

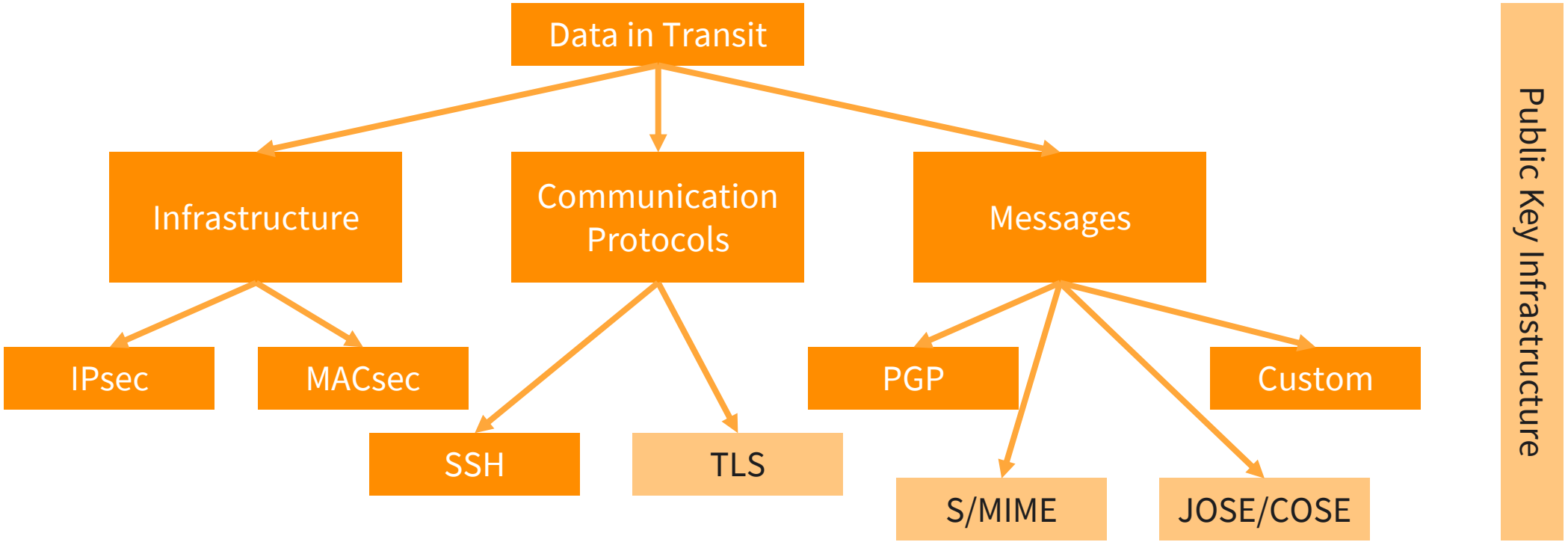
National Institute of Standards and Technology (NIST) recently published:

- **FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)** based on CRYSTALS-Kyber
- **FIPS 204, Module-Lattice-Based Digital Signature Standard** based on CRYSTALS-Dilithium
- **FIPS 205, Stateless Hash-Based Digital Signature Standard** based on SPHINCS+

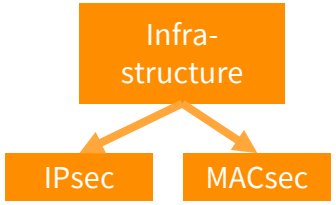
British National Cyber Security Center (NCSC) recommends the NIST standards and hash-based signatures

German Bundesamt für Sicherheit in der Informationstechnik (BSI) recommends conservative algorithms and mentions plans to include the NIST-choices in future versions.

NIST Post-Quantum Cryptography: Digital Signature Schemes competition ongoing



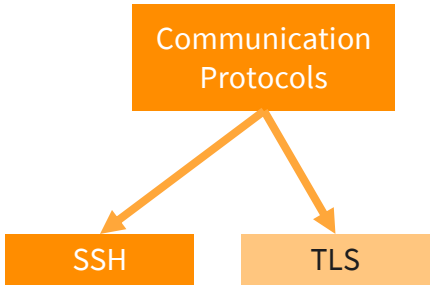
Post-Quantum Cryptography (PQC) required as basis to replace asymmetric algorithms



IPSEC / MACSEC

- **MACsec**
  - relies only on symmetric algorithms during the key agreement
  - key distribution is important

- **IPsec**
  - RFC 8784 use pre-shared keys for post-quantum security
  - Drafts are available for PQC for Internet Key Exchange Protocol Version2 (IKEv2) (individual submissions)



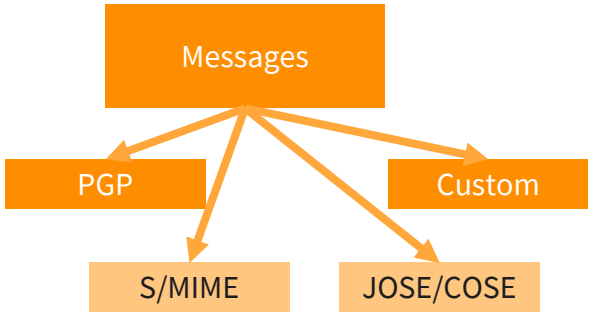
SSH

- **Secure Shell (SSH)**
  - Active IETF drafts for PQC exist
  - OpenSSH uses a PQC key-agreement per default since 9.0/9.0p1
  - AWS implements an IETF draft

Usable implementations for PQC key-agreement exist

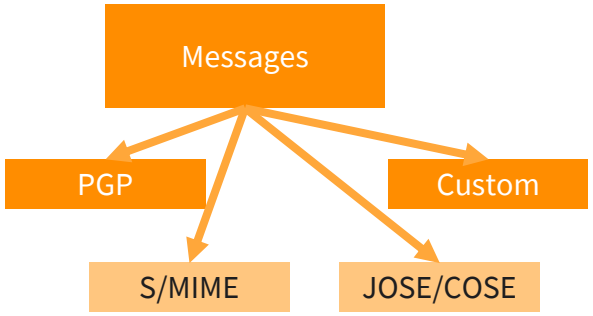
- **Transport Layer Security (TLS)**
  - Focus on TLS 1.3; 1.2 won't be enhanced
  - Various research results on PQC
  - Botan library & OpenQuantum Safe implement hybrid solution (IETF draft) (experimental)
  - Large-scale experiments, e.g. by Google
  - Cloudflare enables PQC support that can be used e.g. with Chrome

Google recently announced their BoringSSL implementation supports ML-KEM and Chrome with switch as well



PGP / S/MIME / JOSE/COSE

- **PGP**
  - IETF draft but lack of practical implementations and experiments
- **S/MIME**
  - PQC on the *Limited Additional Mechanisms for PKIX and S/MIME (lamps)* working group charter
  - Demo Integration for Thunderbird available
- **JOSE/COSE**
  - RFC 8778 defines hash-based signatures for COSE
  - Active IETF and individual drafts exist for PQC support



CUSTOM SOLUTIONS

- **Open Quantum Safe project**
  - Supports transition to PQC
  - Part of the Linux Foundation's Post-Quantum Cryptography Alliance
  - Liboqs: C library for post-quantum algorithms
  - Prototype integration into protocols and applications

Not for use in production

- **Bouncy Castle**
  - Java and C# library including support for different PQC algorithms
  - Recommends using KEM algorithms for short-term protection in a hybrid setting, not for long-term protection

Public Key Infrastructure

Various drafts exists for

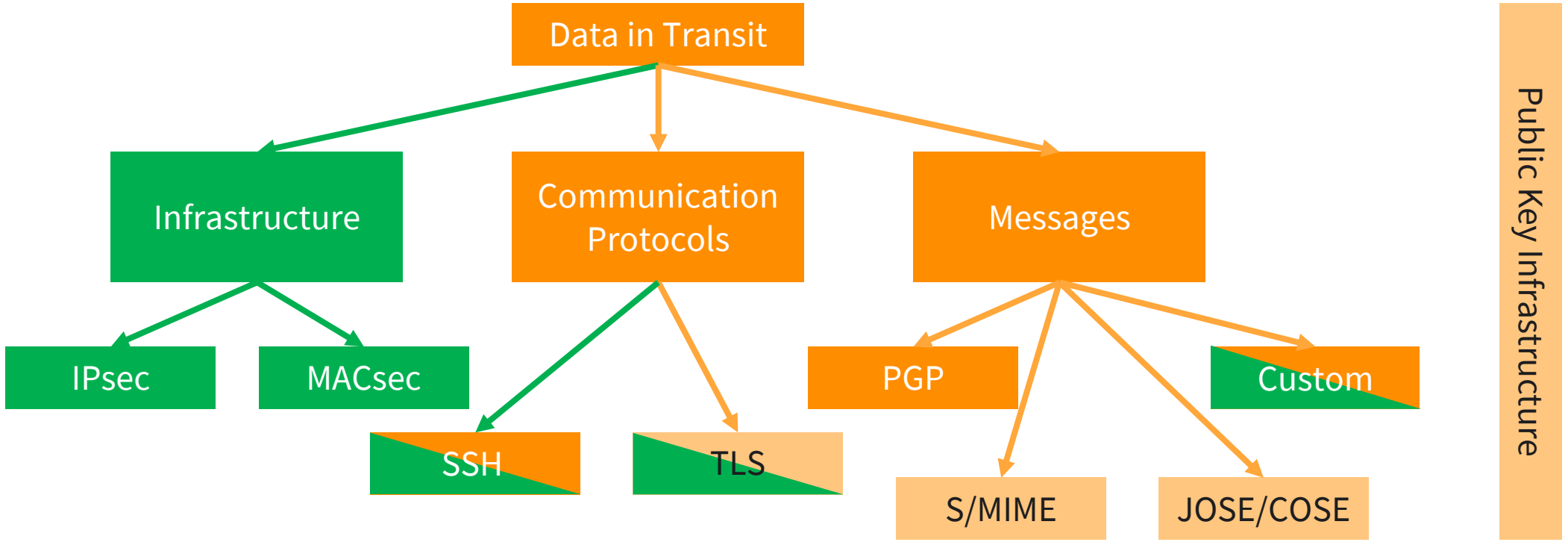
- **PQC Certificates**

- **Composite certificate**
  - Ensure security in case one algorithm is broken

- **Hybrid certificates**
  - Can be verified traditionally in case PQC is not supported

Experimental suites up to solutions are available

CONCLUSION



Post-Quantum Cryptography (PQC) required as basis to replace asymmetric algorithms