TLS and Post-Quantum Cryptography: Securing Communications Today and Tomorrow

Thursday June 1, 2023

intel

XIPHERA

Mark Frost

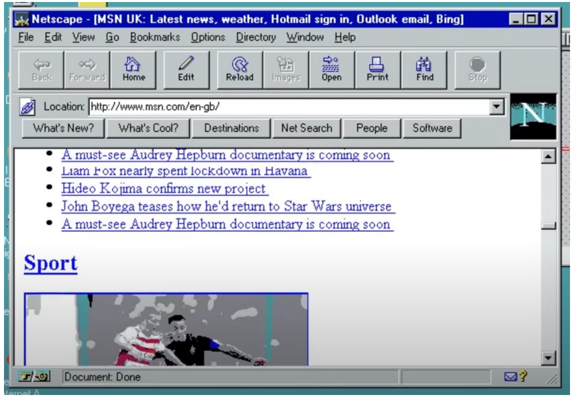
FPGA Security and 5G Technical Marketing Manager, Intel Corporation

Kimmo Järvinen

Co-founder and Chief Technical Officer, Xiphera Ltd.

So what is TLS?

Transport Layer Security (**TLS**) is a cryptographic protocol designed to provide communications security over a computer network. The protocol is widely used in applications such as email, instant messaging, and voice over IP, but its use in securing HTTPS remains the most publicly visible.

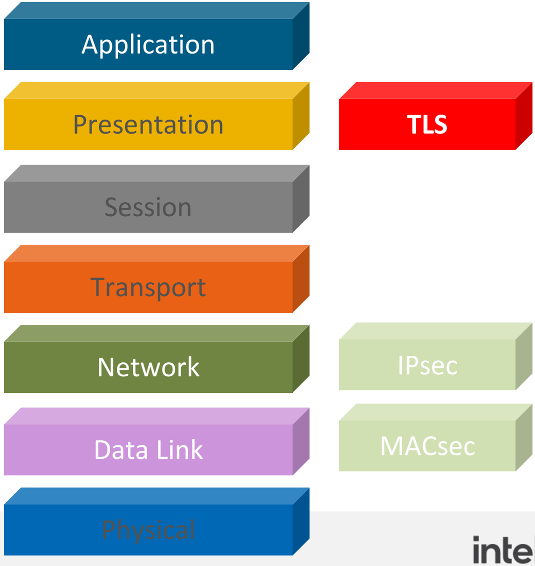

Netscape - [MSN UK: Latest news, weather, Hotmail sign in, Outlook email, Bing]
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Location: http://www.msn.com/en-gb/
What's New? What's Cool? Destinations Net Search People Software

- A must-see Audrey Hepburn documentary is coming soon
- Liam Fox nearly spent lockdown in Havana
- Hideo Kojima confirms new project
- John Boyega teases how he'd return to Star Wars universe
- A must-see Audrey Hepburn documentary is coming soon

Sport

Document: Done

- v1.3 is the latest (defined in 2018)
- Provides confidentiality, integrity and authenticity



How does it work?

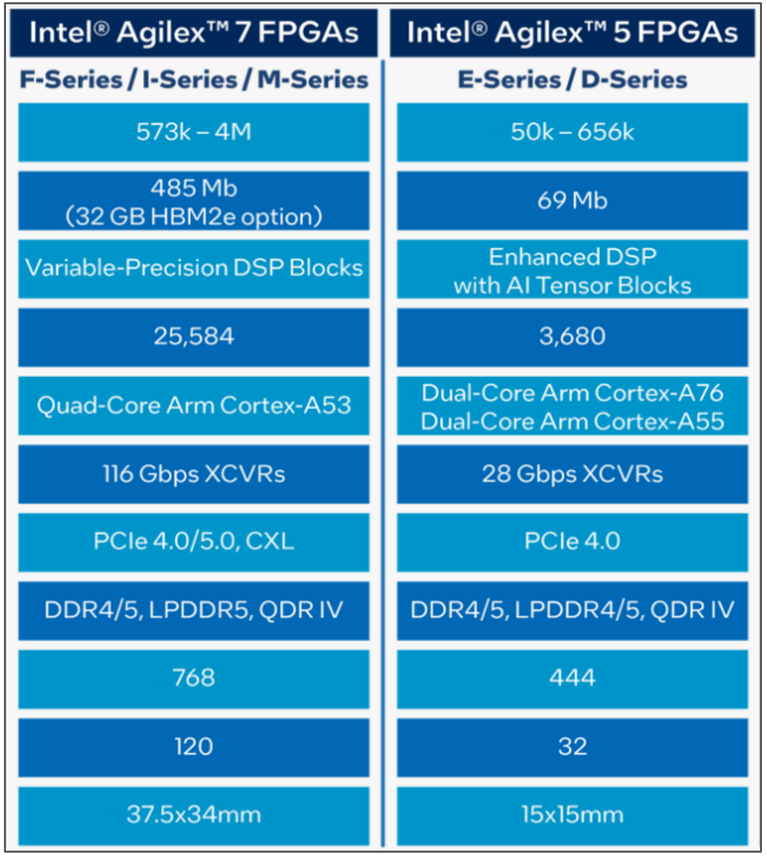
- Client – Server protocol
  - Client requests a secure connection from the server
- Two layers: TLS Record and TLS Handshake. The former defines the message structures, the latter defines how client and server establish a secure session
- Handshake
  - Cipher selection
  - Server authentication (client authentication is also supported)
    - Typically done with digital certificates – PKI
  - Session key exchange – symmetric crypto
- Record
  - Application data records protected for confidentiality and integrity/authenticity
  - Nowadays most typically uses AES-GCM (but also other ciphers supported)

TLS Use Cases – acceleration with FPGA

- NVMe™ over Fabrics (NVMe-oF™) : TCP or RoCE
  - Using a transport protocol over a network to connect remote NVMe devices, contrary to regular NVMe where physical NVMe devices are connected to a PCIe bus either directly or over a PCIe switch to a PCIe bus.
  - FPGA used to accelerate the TCP stack, with TLS on top
- Protecting streaming content
  - Content Service Provided (CSP)
  - Medical
  - Banking
  - Government
  - FPGA accelerates TLS encrypt function (server side)
- High speed Wireline Packet Sniffer
  - End point example

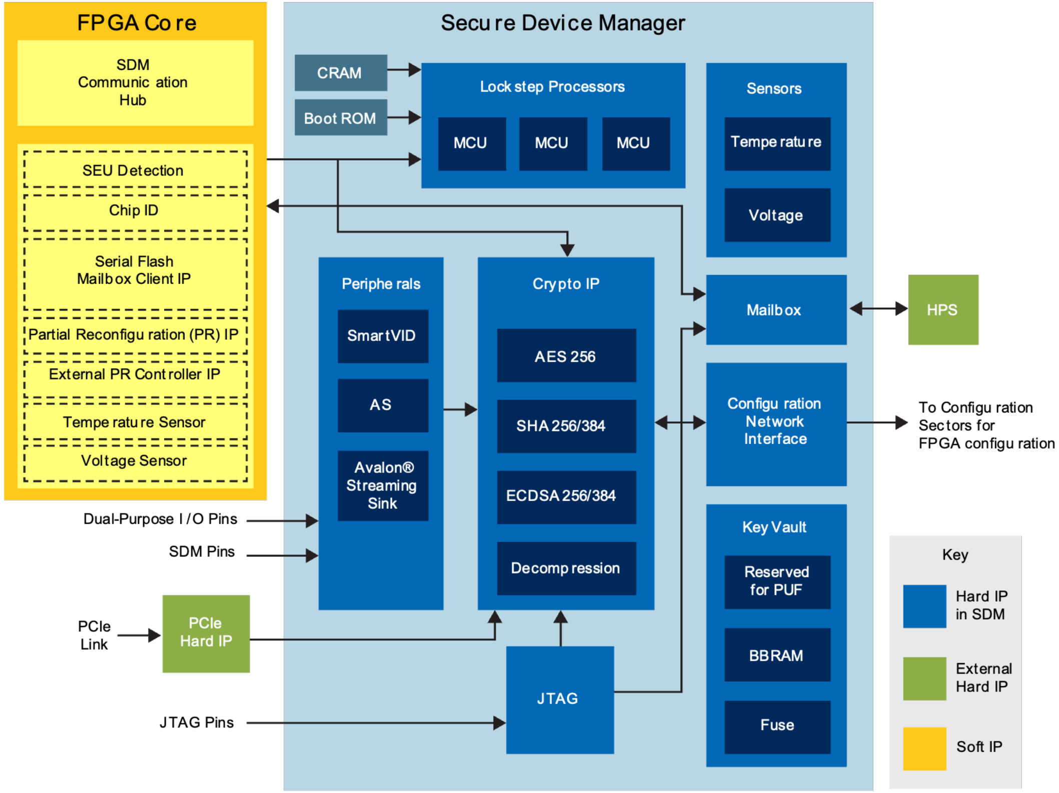
TLS and Intel FPGA ?

Intel has a wide range of FPGAs suitable for TLS implementations



Intel® Agilex™ 7 FPGAs	Intel® Agilex™ 5 FPGAs
F-Series / I-Series / M-Series	E-Series / D-Series
573k – 4M	50k – 656k
485 Mb (32 GB HBM2e option)	69 Mb
Variable-Precision DSP Blocks	Enhanced DSP with AI Tensor Blocks
25,584	3,680
Quad-Core Arm Cortex-A53	Dual-Core Arm Cortex-A76 Dual-Core Arm Cortex-A55
116 Gbps XCVRs	28 Gbps XCVRs
PCIe 4.0/5.0, CXL	PCIe 4.0
DDR4/5, LPDDR5, QDR IV	DDR4/5, LPDDR4/5, QDR IV
768	444
120	32
37.5x34mm	15x15mm

Intel FPGA : Securing your IP and your Data



Agilex FPGAs help secure your design and data from the ground up

Protect your IP

Secure Device Manager in all family members

Secure key vault for TLS

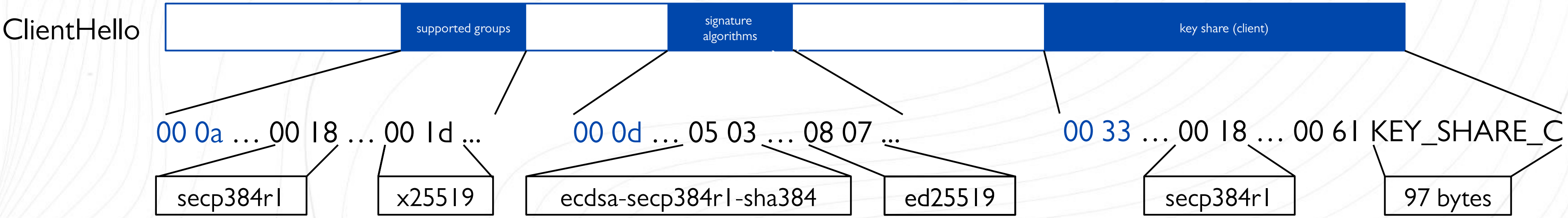
How Does Post-Quantum Cryptography Affect the TLS Protocol?

Kimmo Järvinen

CTO, Co-founder, Xiphera Ltd.

Jun. 1, 2023

TLS 1.3 Handshake



ClientHello

supported groups

signature algorithms

key share (client)

00 0a … 00 18 … 00 1d ...

00 0d … 05 03 … 08 07 ...

00 33 … 00 18 … 00 61 KEY_SHARE_C

secp384r1

x25519

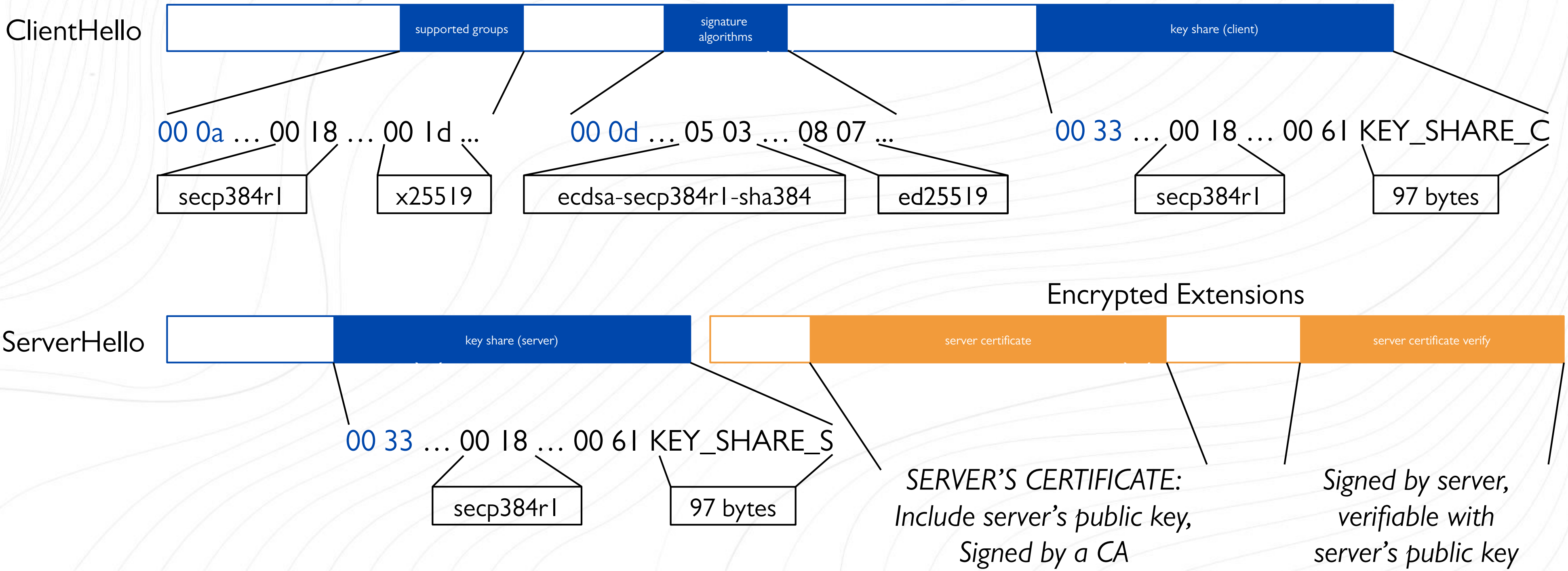
ecdsa-secp384r1-sha384

ed25519

secp384r1

97 bytes

TLS 1.3 Handshake



ClientHello

supported groups

signature algorithms

key share (client)

00 0a … 00 18 … 00 1d ...

secp384r1

x25519

00 0d … 05 03 … 08 07 ...

ecdsa-secp384r1-sha384

ed25519

00 33 … 00 18 … 00 61 KEY_SHARE_C

secp384r1

97 bytes

Encrypted Extensions

ServerHello

key share (server)

server certificate

server certificate verify

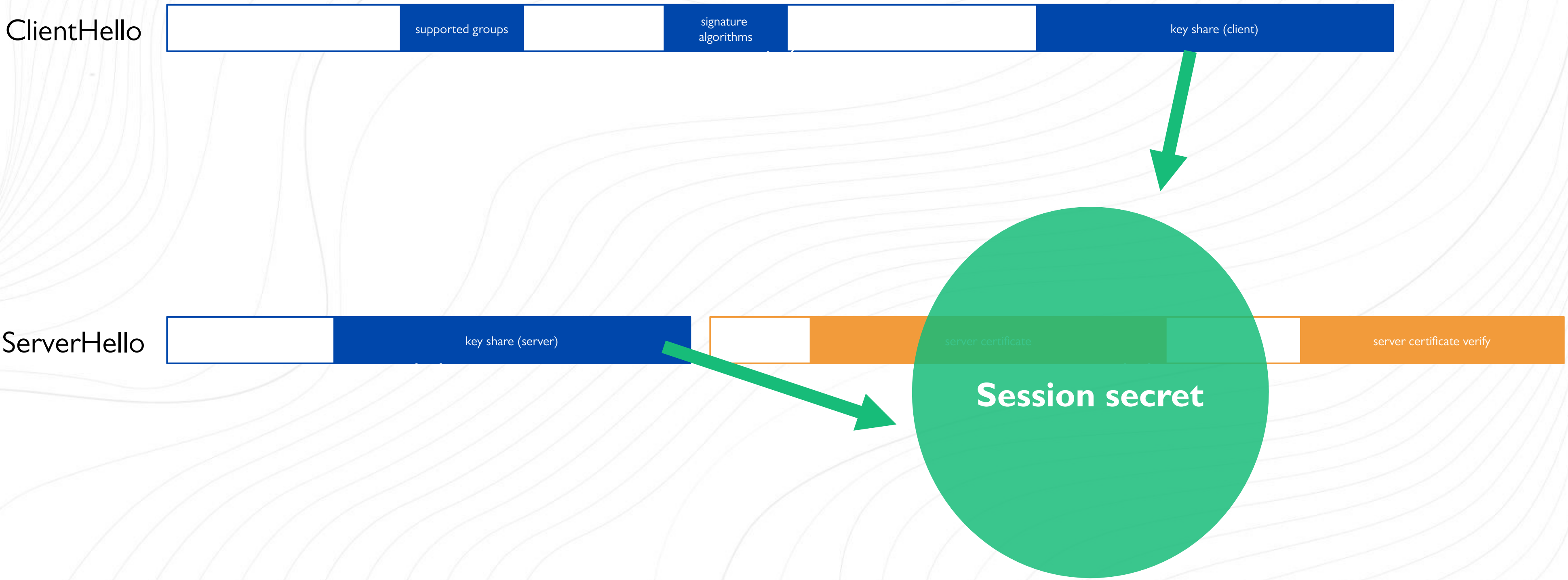
00 33 … 00 18 … 00 61 KEY_SHARE_S

secp384r1

97 bytes

SERVER'S CERTIFICATE: Include server's public key, Signed by a CA

Signed by server, verifiable with server's public key



ClientHello

supported groups

signature algorithms

key share (client)

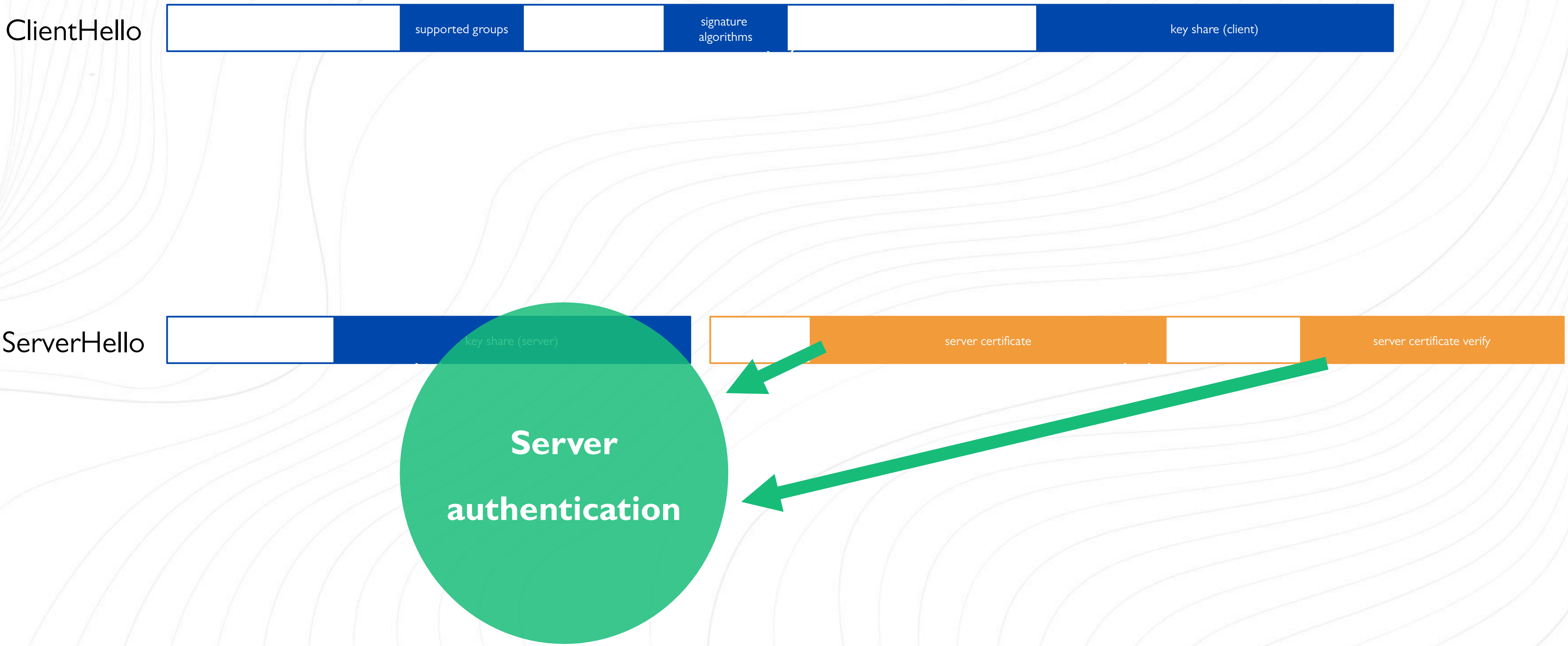
ServerHello

key share (server)

server certificate

server certificate verify

Session secret



ClientHello

supported groups

signature algorithms

key share (client)

ServerHello

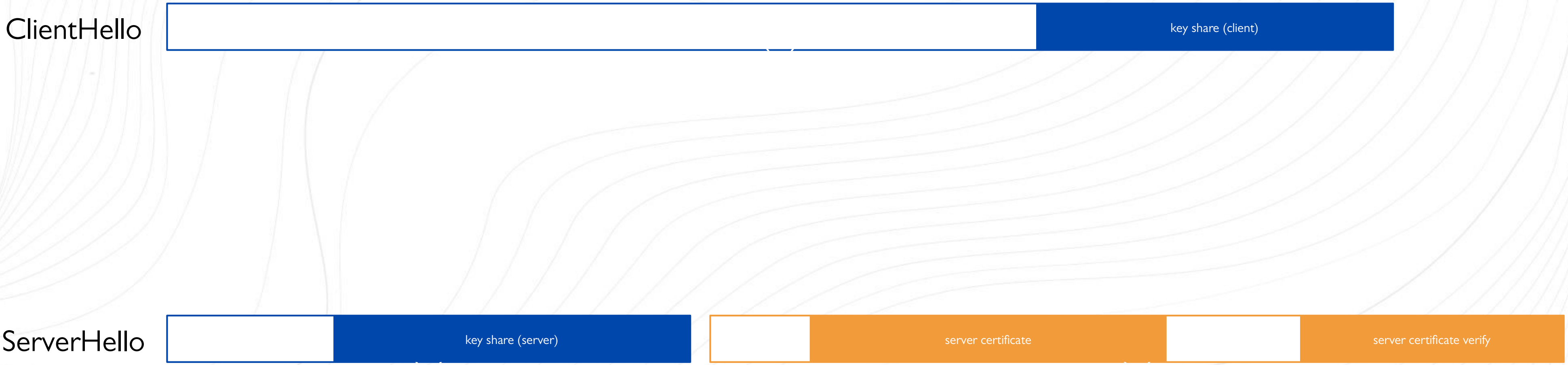
key share (server)

server certificate

server certificate verify

Server authentication

Quantum Targets



ClientHello

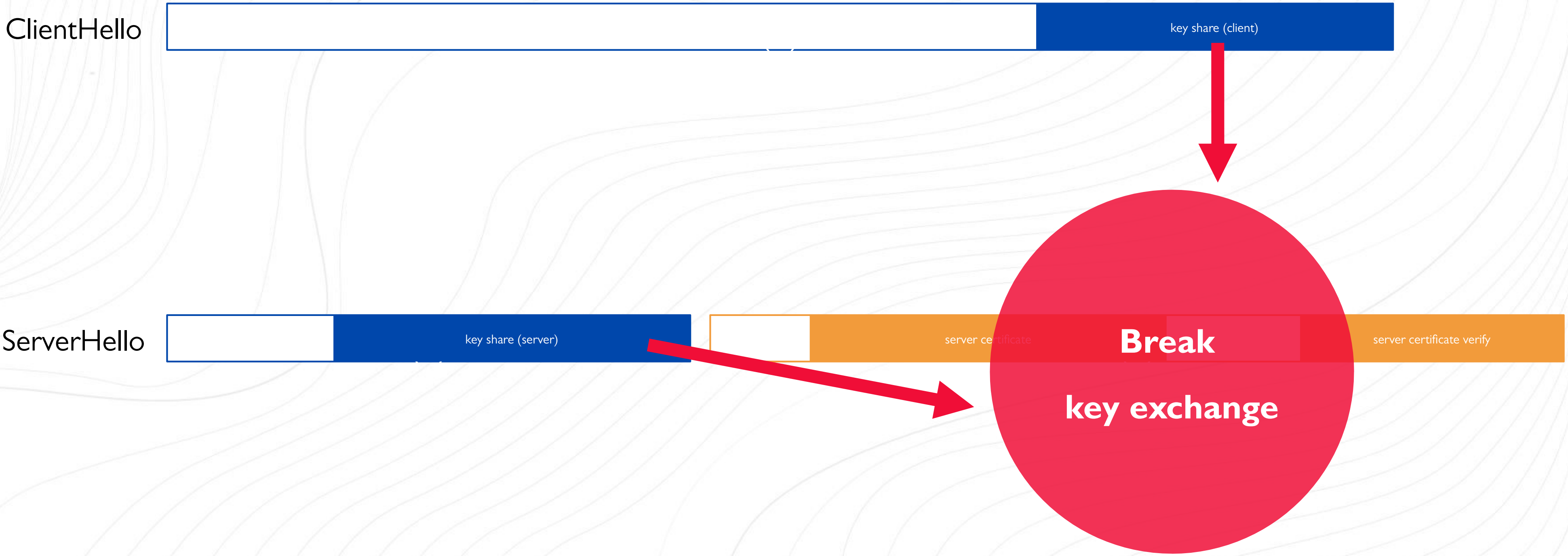
key share (client)

ServerHello

key share (server)

server certificate

server certificate verify



ClientHello

key share (client)

ServerHello

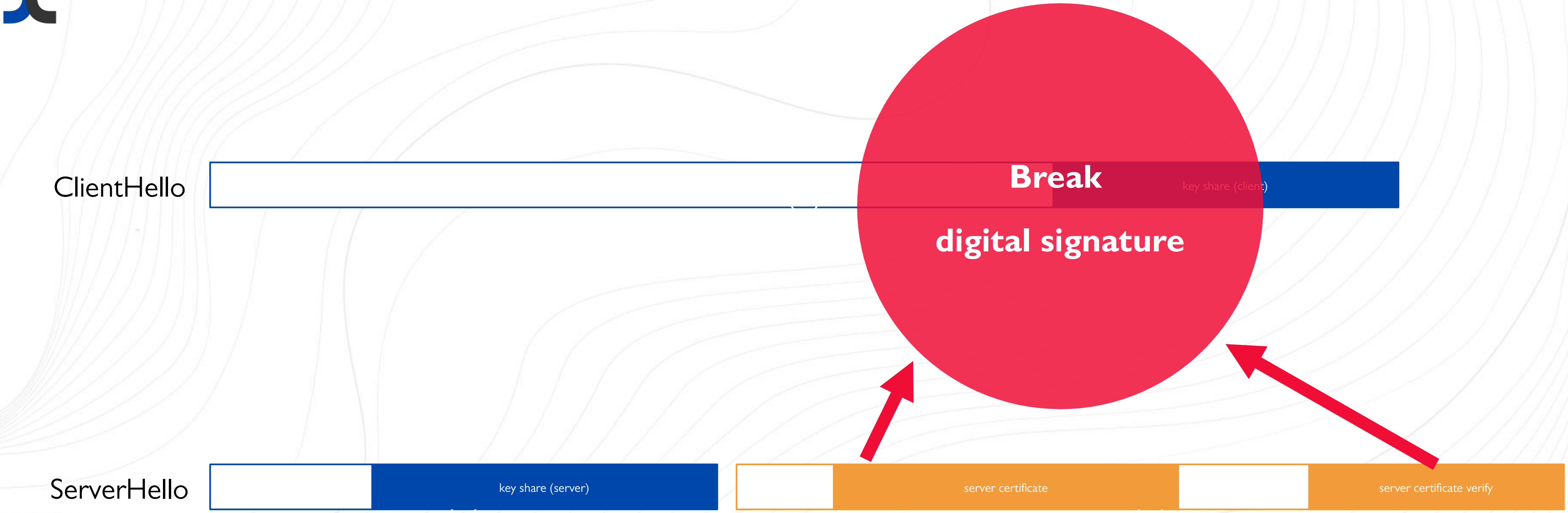
key share (server)

server certificate

server certificate verify

Break

key exchange



Break

digital signature

ClientHello

key share (client)

ServerHello

key share (server)

server certificate

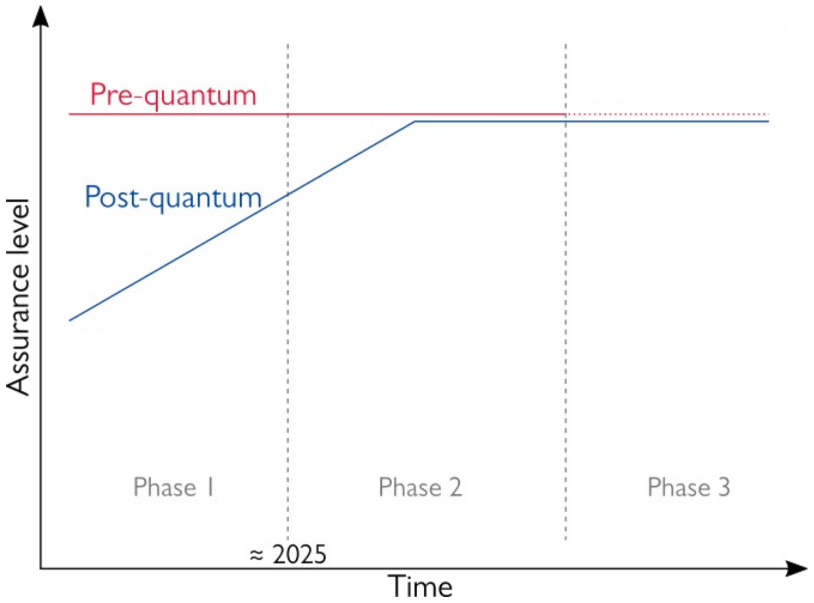
server certificate verify

The Imminent Quantum Threat

- Quantum computers of cryptographic significance do not (probably) exist today!
  - **Record today, break tomorrow**
- TLS *authentication cannot* be broken retroactively
- TLS *key exchange can* be broken retroactively
  - But, each session must be attacked separately!
- **Key exchange must be protected today** if the communication must remain confidential for decades

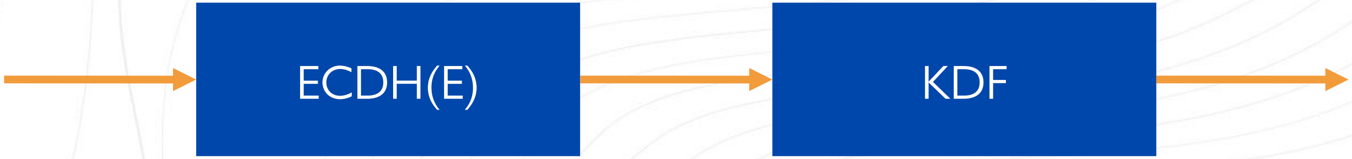
Why Hybrid Systems?

- We cannot fully trust that the new PQC schemes are secure
  - **Example:** NIST finalist Rainbow and Round 4 candidate SIKE were broken!
- Many recommend using a hybrid system
  - ANSSI (France) recommends it at least until 2030
- Elliptic curves will not go away for a long time!

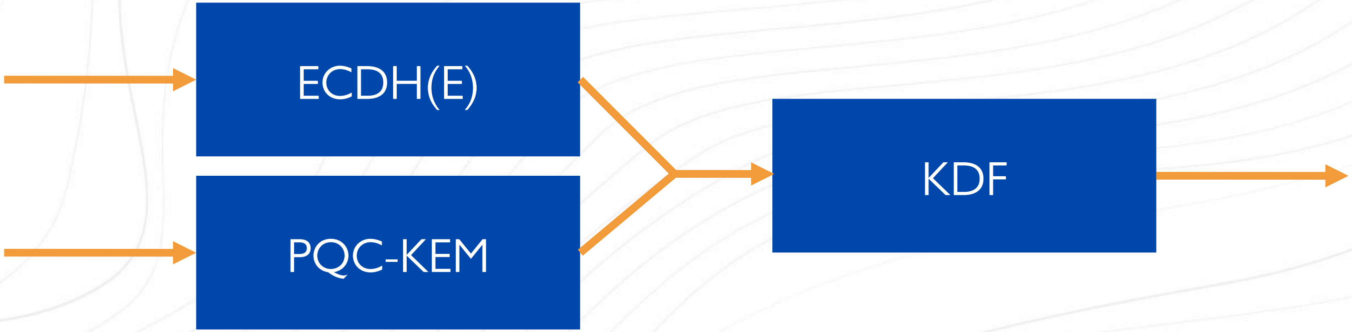


Source: ANSSI (2022)

Hybrid Key Exchange



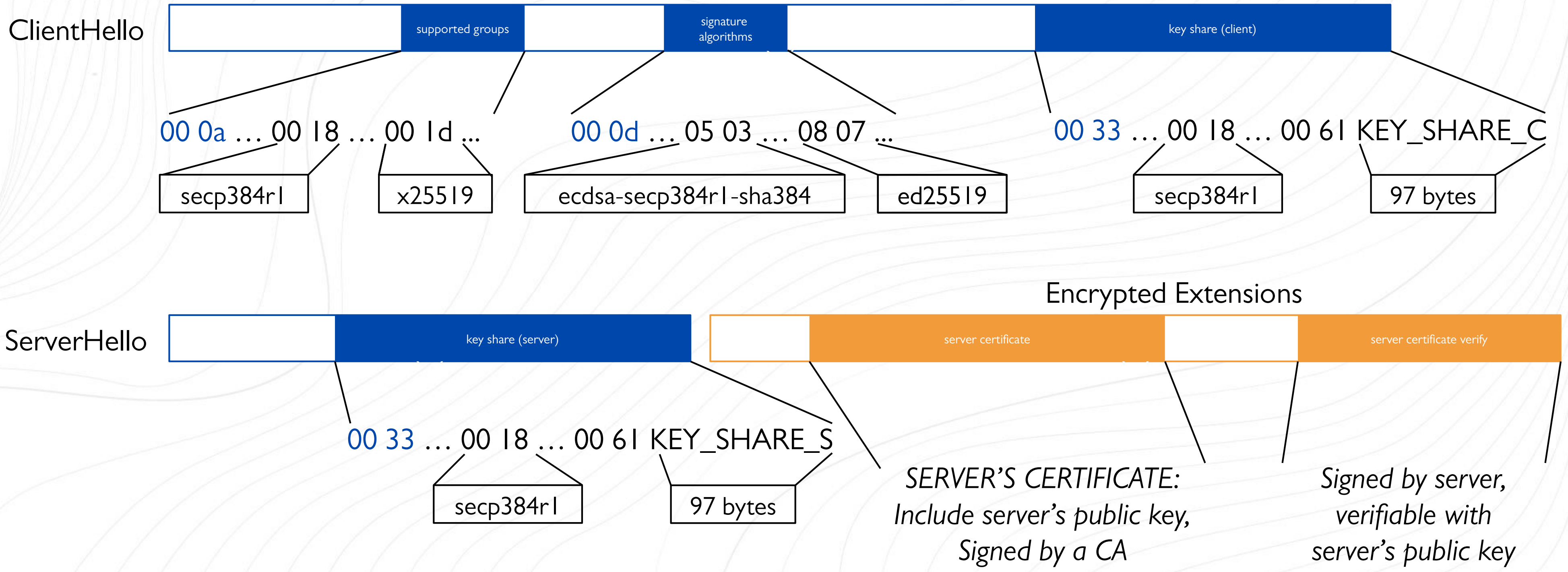
Hybrid Key Exchange



PQ-TLS Proposal

- An internet draft proposes a way to use **hybrid key exchange in TLS 1.3**
- Rather than having two separate "group" and "key share" fields in Client/ServerHello, there is only one; For example,
    - "group": secp384r1_kyber768
    - "key share": Concatenation of secp384r1 key share and kyber768 key share
    - Concatenation of secp384r1 and kyber768 key shares fed into TLS KDF
- The internet draft suggest four hybrid groups, targeted for various use cases

TLS 1.3 Handshake



ClientHello

supported groups

signature algorithms

key share (client)

00 0a … 00 18 … 00 1d ...

secp384r1

x25519

00 0d … 05 03 … 08 07 ...

ecdsa-secp384r1-sha384

ed25519

00 33 … 00 18 … 00 61 KEY_SHARE_C

secp384r1

97 bytes

Encrypted Extensions

ServerHello

key share (server)

server certificate

server certificate verify

00 33 … 00 18 … 00 61 KEY_SHARE_S

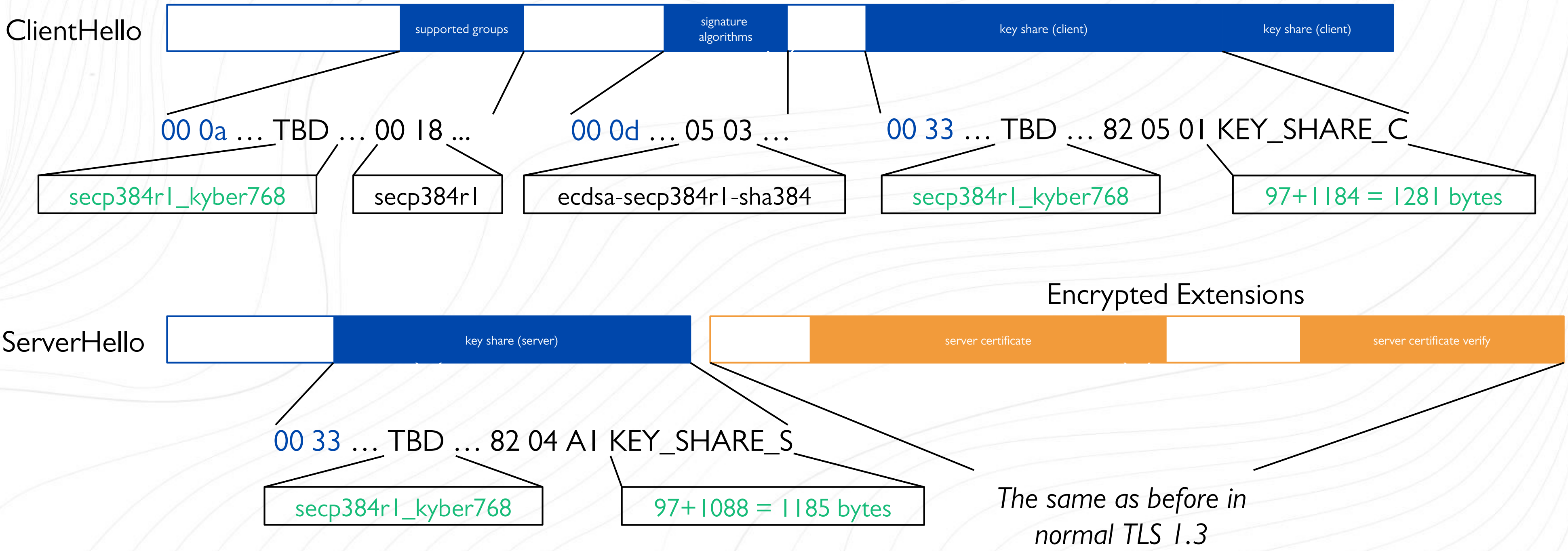
secp384r1

97 bytes

SERVER'S CERTIFICATE:
Include server's public key,
Signed by a CA

Signed by server,
verifiable with
server's public key

PQ-TLS 1.3 Handshake



ClientHello

supported groups

signature algorithms

key share (client)

key share (client)

00 0a … TBD … 00 18 ...

secp384r1_kyber768

secp384r1

00 0d … 05 03 …

ecdsa-secp384r1-sha384

00 33 … TBD … 82 05 01 KEY_SHARE_C

secp384r1_kyber768

97+1184 = 1281 bytes

ServerHello

key share (server)

Encrypted Extensions

server certificate

server certificate verify

00 33 … TBD … 82 04 A1 KEY_SHARE_S

secp384r1_kyber768

97+1088 = 1185 bytes

The same as before in normal TLS 1.3

Xiphera’s TLS and PQC Offering

Transport Layer Security

- Product family extensions announced **today (June 1, 2023)**
- IP cores for both server and client sides
- Implements the whole TLS 1.3
  - Including TLS handshake and session key management
  - Fast performance and high security
- Learn more: xiphera.com/tls.php

xQlave® – Post-Quantum Cryptography

- Product family of efficient implementations of PQC algorithms
- Currently offering
  - CRYSTALS-Kyber (KEM)
  - CRYSTALS-Dilithium (digital signature)
- Learn more: xiphera.com/pqc.php

XIPHERA

Thank you!

www.xiphera.com

kimmo.jarvinen@xiphera.com

mark.frost@intel.com

XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

Cryptography Under the Hood will continue in September!

More info coming soon.

www.xiphera.com

kimmo.jarvinen@xiphera.com

mark.frost@intel.com

References

- IETF: *Hybrid key exchange in TLS 1.3* (https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/06/)