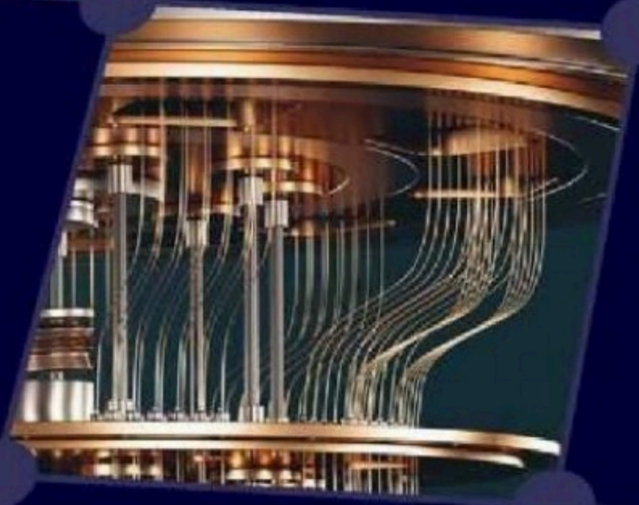
Think openly, build securely

Commercial in Confidence - Copyright PQShield Ltd - All Rights Reserved

# Cryptography evolves… but we're now entering a Quantum Era



Commercial in Confidence - Copyright PQShield Ltd - All Rights Reserved

## Cryptography is a highly standardised technology

- NIST (US) were tasked with starting the process of standardisation of Post-Quantum Cryptography (PQC) in 2016
- Cryptographers are collaboratively solving this problem.

## NIST will announce the new standards around the end of 2021

Commercial in Confidence - Copyright PQShield Ltd - All Rights Reserved

The Quantum Threat

## Impacts the authenticity, integrity and confidentiality of our digital lives

- Our current Cryptography (RSA 1970s, ECC 1980s) is only secure for a few more years, it will be broken by quantum computers - including high risk of retrospective attacks on confidential data
- This affects all cybersecurity infrastructure
- Just check your pockets for all the daily items that use Cryptography:
  - your keys
  - your wallet
  - your phone… to name but a few

Commercial in Confidence – Copyright PQShield Ltd – All Rights Reserved

The change will be mandated

# Government agencies have asked suppliers to get ready for Post-Quantum Cryptography

"...There is growing research in the area of quantum computing, and global interest in its pursuit have provoked NSA to ensure the enduring protection of NSS by encouraging the development of post-quantum cryptographic standards and planning for an eventual transition."

"Post-Quantum Cryptography provides the best mitigation for the quantum computing threat. The NCSC recognises the serious threat that quantum computers pose to long-term cryptographic security. QSC using standards-compliant products is the recommended mitigation for the quantum threat, once such products become available."

# Suppliers need to comply to continue trading

Commercial in Confidence - Copyright PQShield Ltd - All Rights Reserved

# Multiple Drivers for Stronger Crypto

**Cyber warfare** is a reality – Nation-State cyber attacks have doubled in the last three years

Source: HP Research

**Covid-19** has rapidly accelerated digital working and simultaneously heightened security risks - Between February and May 2020 more than half a million people globally were affected by breaches in Video Conferencing, leading **to companies like Zoom** having to rapidly fix significant security flaws

Source: Deloitte

**Hardware is evolving too**: RISC-V rapidly gaining traction as an open source hardware platform – potential to rival ARM and Intel for IoT and Industrial Applications

Source: RISC-V

Commercial in Confidence - Copyright PQShield Ltd - All Rights Reserved

World-Leading Technical Team

# We've built the best team, and growing

+ 2 new starters

## Technical

Our team has so far 13 world class hardware and software cryptography engineers and researchers, with decades of real-world experience, who in turn are attracting more. The team are recruited from the likes of:

arm THALES CLOUDFLARE IBM Radboud Universiteit University of BRISTOL AIST

Commercial in Confidence - Copyright PQShield Ltd - All Rights Reserved

# Experienced Commercial & Advisory Team

## Commercial

Dr Ali El Kaafarani
CEO & Founder

Ben Packman
VP Strategy

Michael Vroobel
VP Operations

Alan Grau
VP Business Dev

## Advisory

Including some of the inventors of modern cryptography

Prof Chris Peikert

Prof Peter Schwabe

Prof Artur Ekert

Commercial in Confidence - Copyright PQShield Ltd - All Rights Reserved

Setting the Standards

# A strategy not a tactic

- NIST PQC Standards
  - We are setting the cryptography standards for the coming decades with NIST, leading multiple final candidates and advising on all of the others – meaning we have excellent visibility over all emerging technologies
- RISC-V Cryptography standards
  - We led the development of the the RISC-V Scalar Cryptography extensions

Commercial in Confidence - Copyright PQShield Ltd - All Rights Reserved

International Recognition

# PQShield established as a reputable Cryptography authority worldwide

- Awards: World Economic Forum Tech Pioneer 2021
- Media: CNBC, BBC, TechCrunch, Forbes, The Telegraph, Business Insider, etc.
- Technical: Our results have been presented at all major security/cryptography events worldwide, including our work with NIST on the new standards

Commercial in Confidence - Copyright PQShield Ltd - All Rights Reserved

Vast opportunity to build now on the new standards about to be finalised

PQShield has unique hardware and software, using standards we helped define and the best crypto talent ever assembled... now is the time...

Commercial in Confidence - Copyright PQShield Ltd - All Rights Reserved

# Browse the best pitch deck examples.

Brought to you by bestpitchdeck.com — the world's largest library of pitch decks: hundreds of winning presentations from leading startups, updated every week.

Read more →

Follow us @pitchdecks