Slide 1

"**The Quantum Elephant in the Room**" is authored and presented by Wolfgang Flatow; Quantum Security Analyst and Inventor of FES.

Wolfgang is an IT professional, Systems Analyst and Enterprise Systems Architect with over 40 years of industry experience.
He is the inventor of patented **Fractal Transformation** that has been researched, refined and developed to production stage as the Fractal Encryption Standard (**FES**).
FES was found to be impenetrable by any computational means, including Quantum Computers.
This led to his investigation of Quantum Computing and its threat to all classic encryption, including AES.
His Quantum Computer analysis since 2021 has yielded 5 different Quantum Algorithms capable of extracting keys from AES ciphertext. These have been further refined and verified by several AI engines including ChatGPT and Grok3.
He has coined the term "Quantum Key Extraction", or QKE, to describe the threat.

This presentation is a summary of Wolfgang's QKE findings.

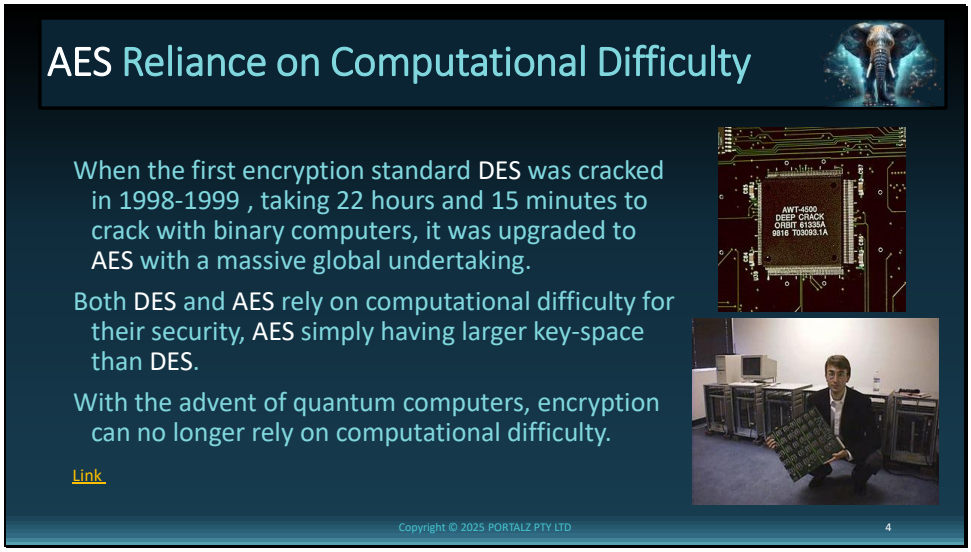
Slide 2

There is a huge "**Quantum Elephant in the Room**" !
It is real, present and dangerous, yet it's presence is not acknowledged.
We will here do our best to reveal that Quantum Elephant.

Slide 3

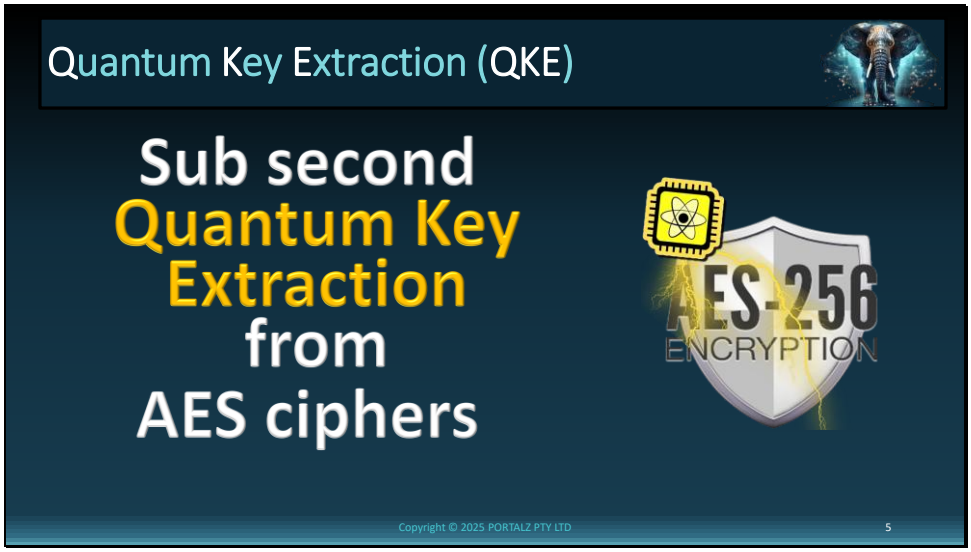
The magnitude of the threat of Quantum Computers to encryption, the foundation of all cybersecurity, cannot be overstated.
Quantum Computer Decryption is the cause of an imminent global Cybersecurity Extinction Level Event.

Slide 4



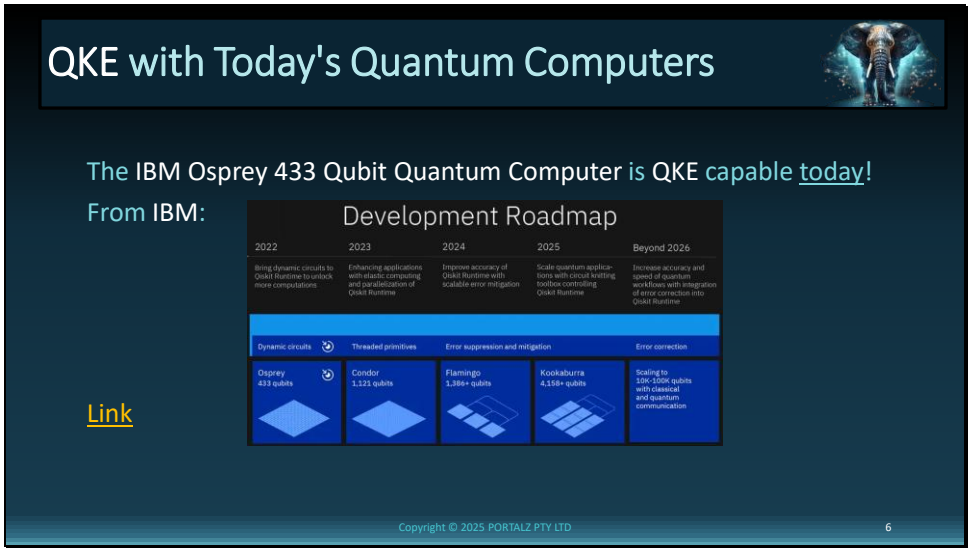
When the first encryption standard DES was cracked in 1998-1999 , taking 22 hours and 15 minutes to crack with binary computers, it was upgraded to AES with a massive global undertaking.
Both DES and AES rely on computational difficulty for their security, AES simply having larger key-space than DES.
With the advent of quantum computers, encryption can no longer rely on computational difficulty.

Slide 5



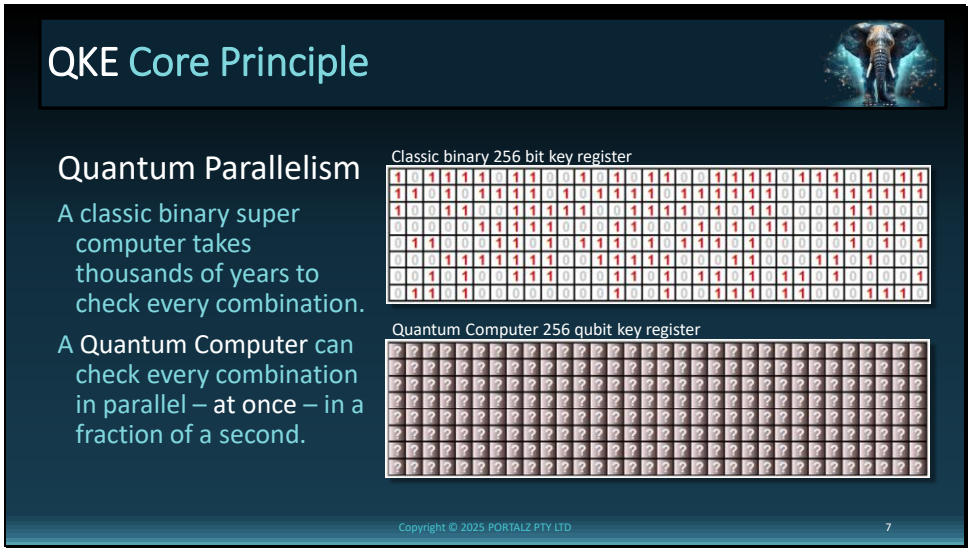
The core of the threat is called Quantum Key Extraction, or QKE.
QKE is the capacity of Quantum Computers to extract the key used to encrypt payload from the ciphertext it generated.
The revolutionary parallel processing power of quantum computers can extract the key in a fraction of a second, compared to thousands of years for conventional binary computers.

Slide 6



Importantly, QKE can be accomplished with today's quantum computers.
A reason for cybersecurity industry complacency in regards to the quantum security threat is an erroneous assumption that today's quantum computers are not powerful enough to threaten encryption and that this threat lies decades in the future.
We have confirmed that the IBM Osprey 433 qubit Quantum Computer, available since 2022, is QKE capable.

Slide 7

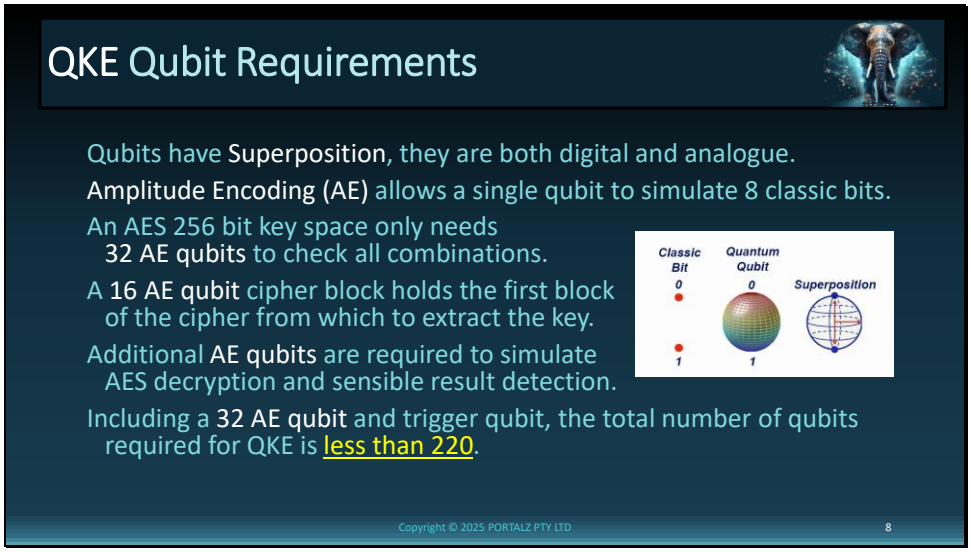


Here is the core principle behind **QKE**.

Where classic computers use bits to process data, quantum computers use qubits.
The classic binary key register diagram shows 256 bits that can be either 0 or 1. It shows one of 2^256 possible bit combinations. In order for a classic computers to process all 2^256 possible bit combinations takes classic computers thousands of years.

In contrast, the quantum computer key register diagram shows 256 qubits that can be both 0 and 1 at the same time. That is a remarkable and seemingly impossible feature of qubits.
When the 256 qubits are quantum entangled they can process all 2^256 possible combinations at once – in a fraction of a second!

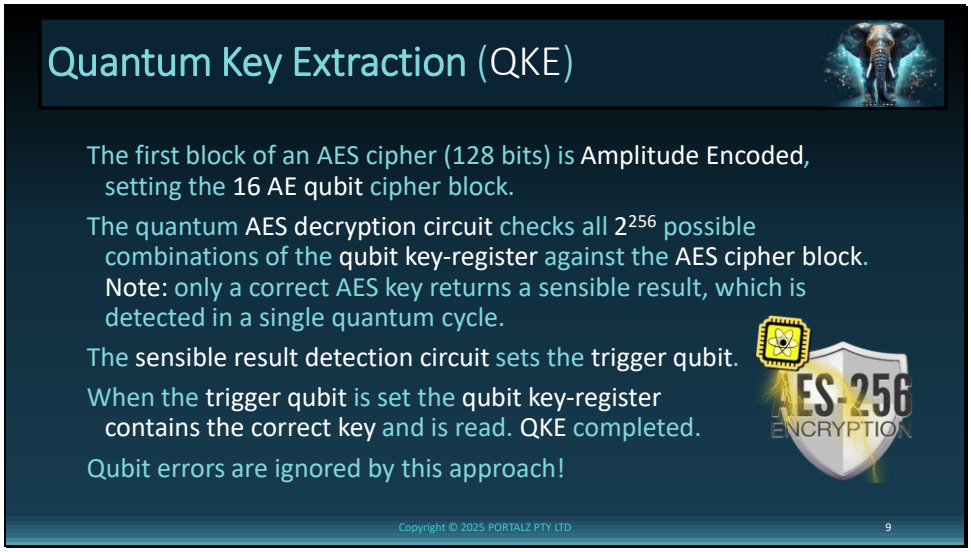
Slide 8



Another remarkable property of qubits is that they can not only be 1 and 0 at the same time, qubits can also be a fraction between 0 and 1 at the same time – an analog processing capability called Superposition.
Initially superposition always collapsed to 0 or 1 when measured, matching classic bits.
Now we can also read and write fractional qubit values using a system called **Amplitude Encoding,** allowing us to simulate multiple bits with a single qubit.
To simulate 8 bits the qubit amplitude (fractional) range is divided into 256 fractions between 0 and 1.
That means we only need 32 qubits to simulate 256 bits, the maximum AES key size.
It also means that the number of qubits required for quantum decrypt simulation is reduced by a factor of 8.

The delivers comprehensive AES-256 QKE quantum decryption algorithm to requiring less than 220 qubits.

Slide 9



By combining **Amplitude Encoded** qubits, a **quantum entangled qubit key-spac**e and **quantum decrypt simulation algorithms** we can build a full **QKE** system.

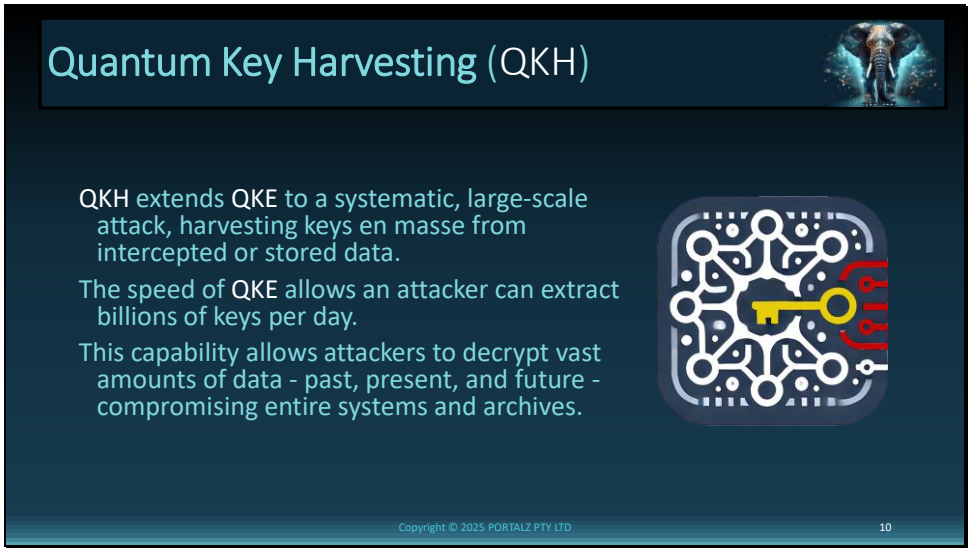
The first block of an AES cipher (128 bits) is Amplitude Encoded, setting the 16 AE qubit cipher block.
The quantum AES decryption circuit checks all 2^{256} possible combinations of the qubit key-register against the AES cipher block.

Note:
only a correct AES key returns a sensible result, which is detected in a single quantum cycle.

The sensible result detection circuit sets the trigger qubit.
When the trigger qubit is set the qubit key-register
contains the correct key and is read. QKE completed.

Importantly; Qubit errors are ignored by this approach, which means that no additional qubits are required for error correction.

Slide 10



QKH extends QKE to a systematic, large-scale attack, harvesting keys en masse from intercepted or stored data.
The speed of QKE allows an attacker can extract billions of keys per day.
This capability allows attackers to decrypt vast amounts of data - past, present, and future - compromising entire systems and archives.

Slide 11

It is no exaggeration that QKE utterly collapses the full security stack, the entire cryptographic foundations securing the world's data, communications and cybersecurity infrastructure.

The ability to quantum brute-force the key from an AES cipher bypasses all key security technologies such as key management (KM), secure key storage, Trusted Platform Module (TPM) hardware key vault and public/private key exchange (RSA).

Slide 12

While quantum computers are promoted for their capabilities for benign R&D, they are a strategic weapon in the information war.

Quantum Computer Decryption of AES, RSA and all classic encryption algorithm has been a significant impetus for their development.
It can be argued that decryption is their primary strategic purpose, value and the driver of their seemingly unlimited state funding.

QKE is a significantly greater threat than Quantum Decryption because, once the key is extracted, classic binary computers can extract the payload.

The key is valid for the whole session, document or multiple files, folders, databases...

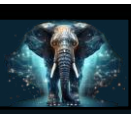
There are clear indications that QKE is already weaponised by intelligence and defence.

Slide 13

The speed and versatility of QKE means it exposes AES secured content in real time.
Armed with QKE an attacker can instantly access the original document or transmission plaintext as it is transmitted.
QKE is available wherever an attacker has access to quantum computers.
Quantum computers capable of running QKE are proliferating globally.

Slide 14

Cloud App Extinction

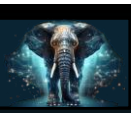


AES/RSA reliant Apps must be withdrawn. Say goodbye to:

- Online Banking and touch payments (no transaction or account security)
- Online Shopping, sales, eBay, Etsy, Amazon etc (no account security)
- All online services that require a login (no account security)
- Government online services (no account security)
- Company, patent and trademark online services (no account security)
- Social Media, Facebook, X, Tik-Tok etc (no account security)
- VPNs and online privacy services

Slide 15

Corporate Intranet Extinction

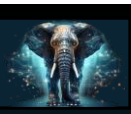


Corporate intranets have greater firewall protection, yet all internal data and communications security remains undermined by QKE:

- Any intranet breach instantly escalates to full QKE compromise.
- Any compromised staff can extract keys at will directly from encrypted files, documents and communications via QKE.
- Any key management/vault/database systems that secure keys via AES can be compromised in seconds with QKE.
- Weaponised AI with quantum computer access can recursively crawl an entire corporate intranet and extract all keys in minutes.

Slide 16

National Security Suppression



AES is the **Advanced Security Standard** as recommended by NIST and mandated by the US Government.

Subsequently every US department, Agency, Contractor and Service Provider has adopted AES for their encryption to remain compliant.

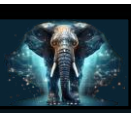
Further, most nations have followed suit in order to be compliant with US security mandates.

When AES is compromised, which is the case with QKE, that means US national security is compromised, along with the national security of all nations who have adopted and mandated AES.

National Security must suppress any AES compromise, including QKE.

Slide 17

Military & Defence Compromise



US Military and Defence all use AES.

The only difference from civilian usage is key-size. From Wikipedia:

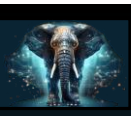
"The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths."

That was true before the advent of quantum computers.

QKE is logically proven to extract keys of 128, 192 and 256 bit keys since the release of the IBM Osprey 433 Qubit QC released in 2022.

Slide 18

Harvest Now – Decrypt Later



From Wikipedia:

"**Harvest now, decrypt later** is a surveillance strategy that relies on the acquisition and long-term storage of currently unreadable encrypted data awaiting possible breakthroughs in decryption technology that would render it readable in the future – a hypothetical date referred to as Y2Q or Q-Day.

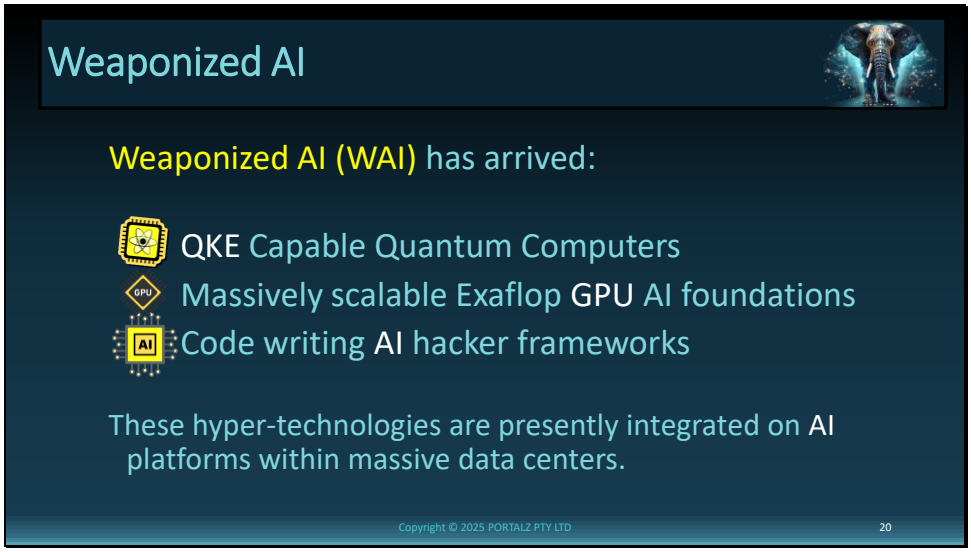
The most common concern is the prospect of developments in quantum computing which would allow current strong encryption algorithms to be broken at some time in the future, making it possible to decrypt any stored material that had been encrypted using those algorithms."

QKE means; that 'future' is NOW!

Slide 19

The misconception that the quantum threat is decades away is prevalent in the cybersecurity industry.
This complacency is a result of focusing on public key encryption, RSA, that requires thousands of error corrected qubits.
The quantum threat to AES has been ignored due to a belief that AES-256 is quantum resistant with quality keys.
As we have shown, AES is much more vulnerable to quantum attack than RSA.
The threat to AES is clearly present with today's Quantum Computers, QKE is possible NOW!
And QKE bypasses RSA key-exchange security.

Slide 20

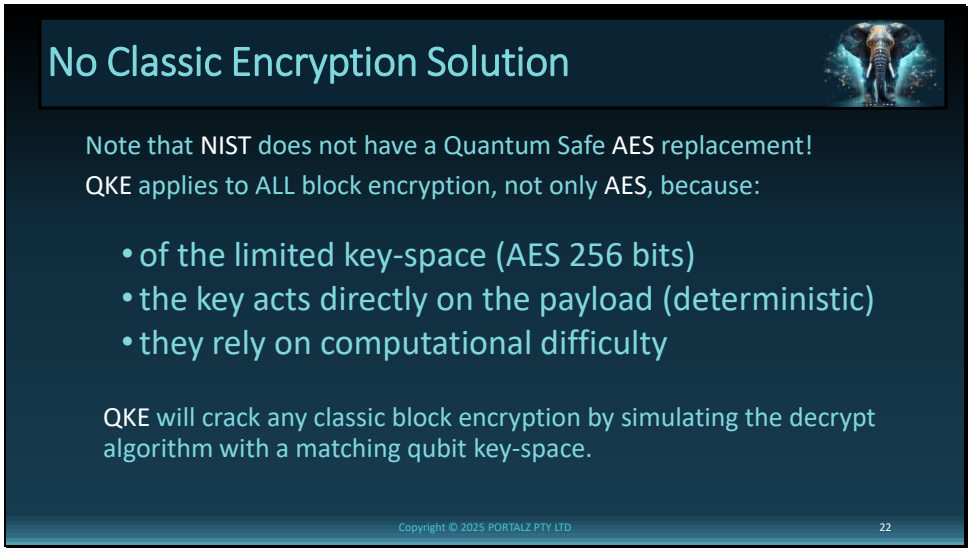


QKE capable Quantum Computers now exist at the core of Weaponized AI Platforms.
Augmented by massively parallel exaflop GPUs (Nvidia GB200 NVL72), Quantum Computers are able to be leveraged by dynamic recursive self-programming and hacker code writing.
This is the perfect Cybersecurity Storm!

Slide 21

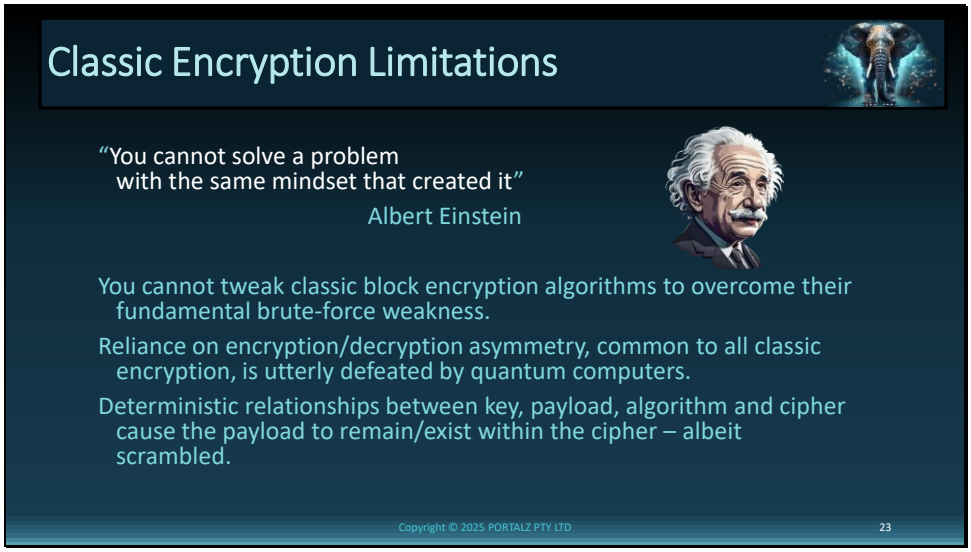
The Quantum Elephant in the Room is in reality a Quantum Stampede in the Room.
QKE is dramatically leveraged by the existence of Weaponized AI.
This hybrid threat exists NOW and should be the focus of every cybersecurity organisation.

Slide 22



QKE core principles apply to every classic encryption algorithm.
NIST does not have/offer a solution because no classic approach works.

Slide 23



All classic encryption relies on brute-force computational difficulty for its security. Quantum Computers crack all classic encryption.

Slide 24

We have passed the QKE point of no return. All encryption is compromised NOW!

Slide 25

AES is Quantum Toast.

That is the Quantum Elephant in the Room.

A quantum hacker will read your email, Telegram Chat, all encrypted communications.
All encrypted internet traffic, including usernames, passwords, sessions, application data, etc are cracked by QKE.

Three level authentication is useless as the subsequent session traffic is decrypted in real time...

It is a present Cybersecurity Extinction Level Event
that the cybersecurity industry thinks is decades away…

Slide 26

Thank you for watching this presentation.

For Quantum-Proof Solutions visit https://portalz.solutions.