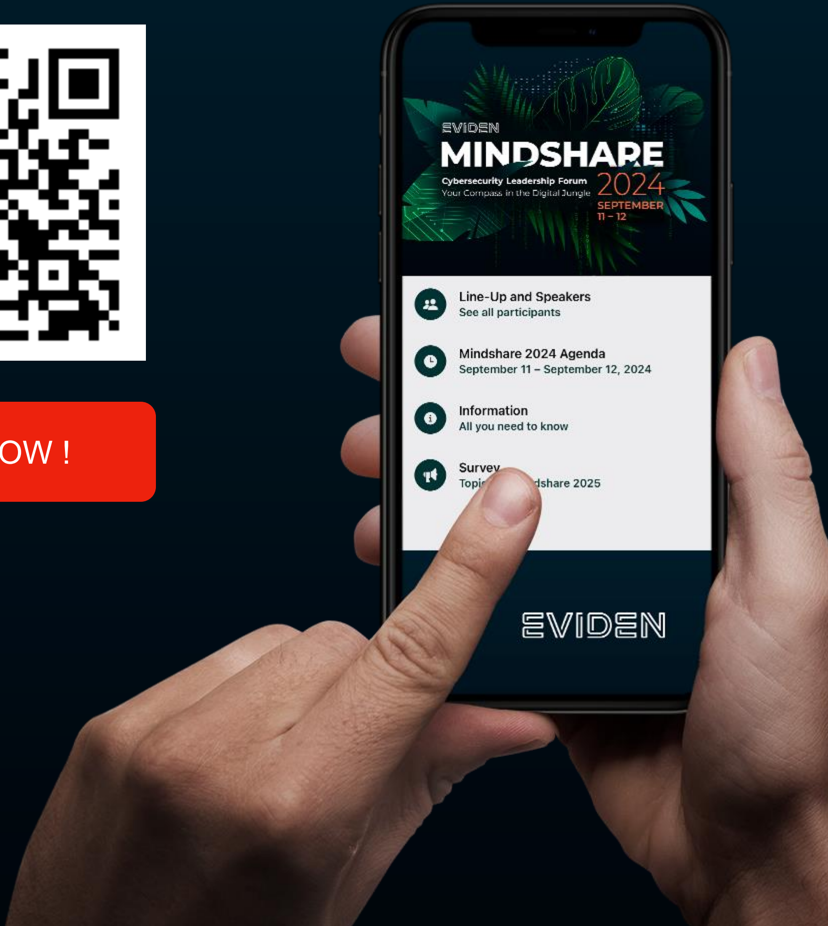
# MINDSHARE 2024 AGENDA

SCAN NOW !



QUANTUM DICE

# The Vital Role of Randomness in Cybersecurity (and What Happens When It Fails)

True Randomness.

# The Problem

## WHAT IS RANDOM?

8 9 7 9 3 2 3 8 4 6 2 6 4 3 3 8 3 2 7 9

Can you predict the next digit?
They look pretty random, right?

# The Problem

## WHAT IS RANDOM?

3 . 1 4 1 5 9 2 6 5 3 5 8 9 7 9 3 2 3 8 4 6 2 6 4 3 3 8 3 2 7 9

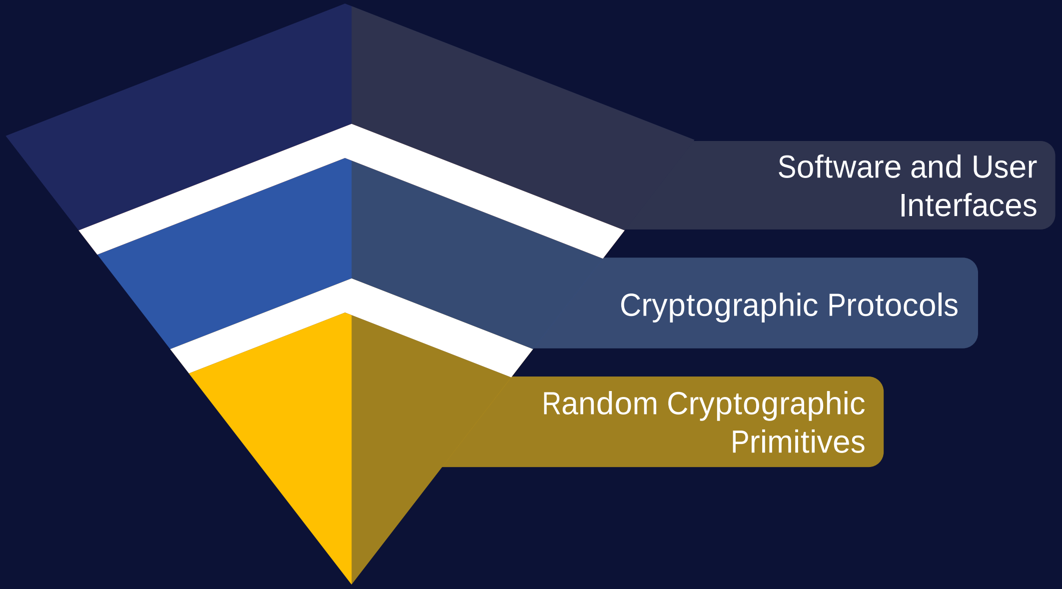
How about now?

It’s just consecutive digits from the number π

Completely predictable with a mathematical formula

# The Problem

## RANDOMNESS IS ESSENTIAL



# The Problem

## SECURE RANDOMNESS IS HARD

Chronology of Failure of Modern RNGs

- 2008 — Debian OpenSSL RNG failure
- 2012 — Compromised RSA keys on embedded devices
- 2013 — Taiwan Smart Card Randomness Vulnerability
- 2019 — Cisco ASA low entropy keys vulnerability
- 2023 — Cisco ASA low entropy keys vulnerability (again)

QUANTUM DICE

# The Problem

## CONNECTIVITY ➔ VULNERABILITIES

### Key Infrastructure

Power grid and government systems are constantly targeted by cyber warfare.

### Communications Networks

Handle everything from online payments to secure messaging and networking systems.

### Private Data

All our personal information from medical records to credit history is vulnerable to security leaks.

*Global average cost of a data breach was $4.88M in 2024*

IBM Data Breach Report

# Advances in the Cryptographic Stack

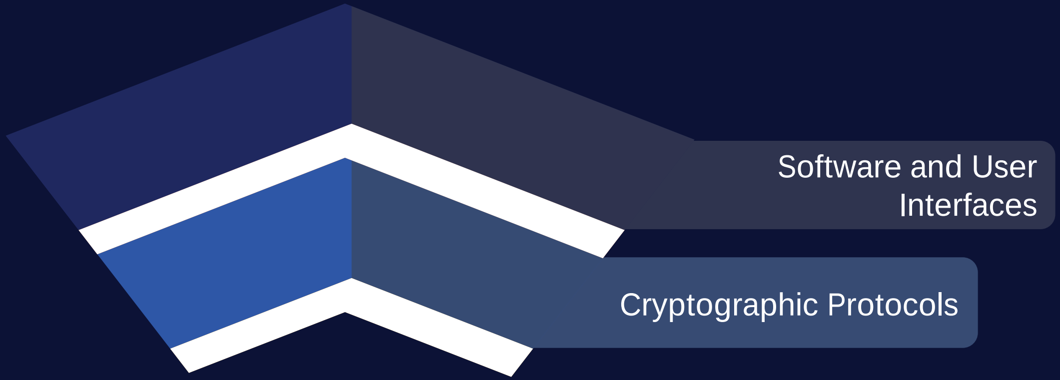
Software and User Interfaces

Post-Quantum Encryption

New Algorithms to resolve vulnerabilities that would be cause by the advent of Quantum Computers

Post-Quantum ≠ **Quantum**

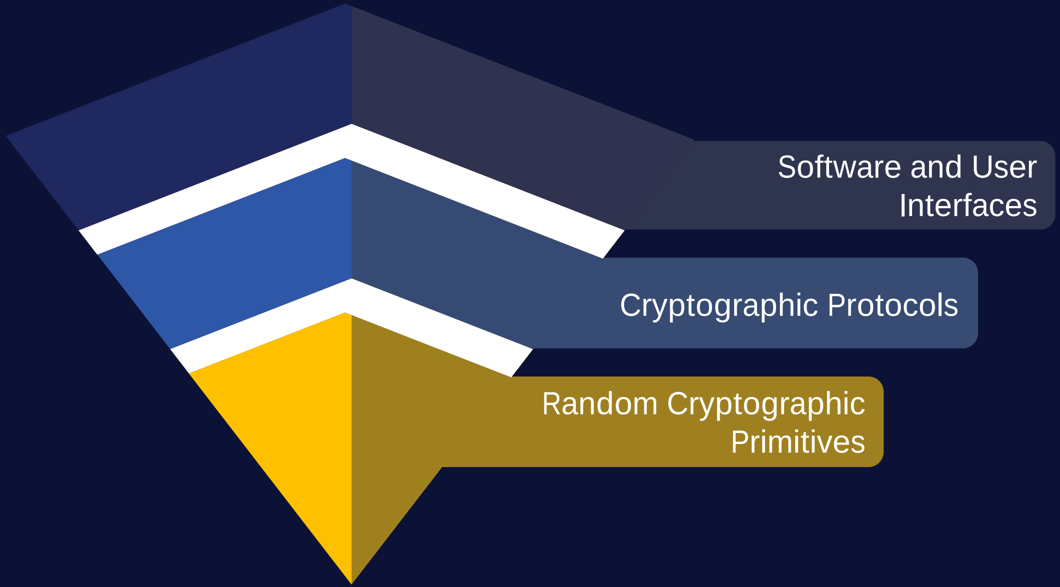
# Advances in the Cryptographic Stack




**Quantum Key Distribution**

Using quantum properties to send and exchange encryption keys securely

# Advances in the Cryptographic Stack




Randomness Remains Essential



QUANTUM DICE

# Understanding Randomness

Pseudo-Random Number Generators

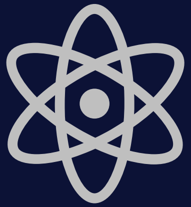
Software-based

Inherently deterministic

Classical True Random Number Generators

Hardware-based

Randomness is easily biased



Quantum Random Number Generators

Hardware-based

There are no perfect quantum systems in practice

*"Anyone who attempts to generate random numbers by deterministic means is, of course, living in a state of sin."*

John Von Neumann

QUANTUM DICE

# Understanding Randomness

- Randomness isn’t a binary property (no pun intended)
- Processes can be more or less random

Which of these is more random?

# Understanding Randomness

- What is Entropy?
  - Given a process $X$ that produces a range of outputs $x_i$, each with a probability $p_i$, a measure of the general unpredictability of that process can be defined
  - Entropy can refer to many different concepts from information theory which try to define unpredictability in different way
  - The two most well-known definition is the Shannon entropy and the min-entropy which are respectively:

$$H_2(X) = -\sum p_i \log_2 p_i \qquad\qquad H_\infty = -\log_2 \max_i p_i$$

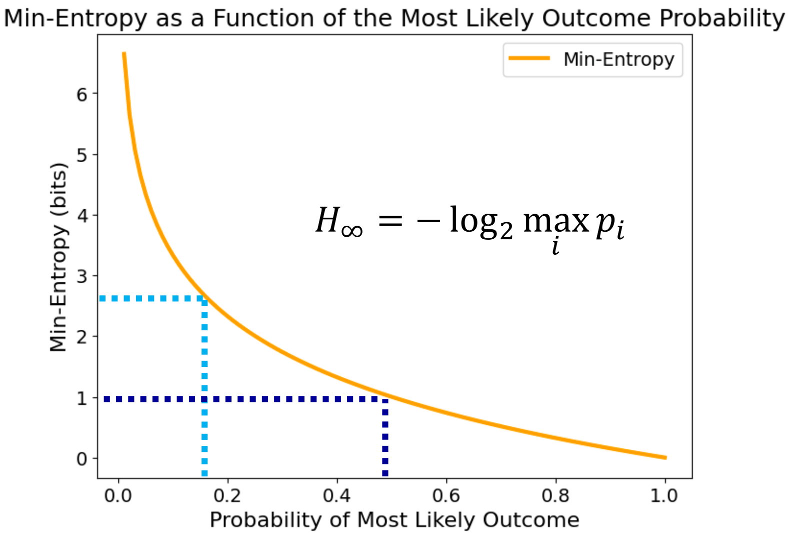
# Understanding Randomness

- What is Entropy?
  - Given a process $X$ that produces a range of outputs $x_i$, each with a probability $p_i$, a measure of the general unpredictability of that process can be defined
  - Entropy can refer to many different concepts from information theory which try to define unpredictability in different way
  - The two most well-known definition is the Shannon entropy and the min-entropy which are respectively:

$$H_2(X) = -\sum p_i \log_2 p_i \qquad\qquad H_\infty = -\log_2 \max_i p_i$$

- How is this used?
  - Min-entropy is the fundamental metric used in the theory of randomness extraction, as such it's the main way one can assess the randomness of a process
  - Based on the min-entropy of a process, randomness extractors can be used to produce a uniformly distributed random output from that process
  - Every element in the cryptographic stack relies on a trusted assessment of the entropy

# Understanding Randomness




$p = 0.5$

$H_\infty = 1$ bit

$p = 1/6$

$H_\infty \approx 2.6$ bits

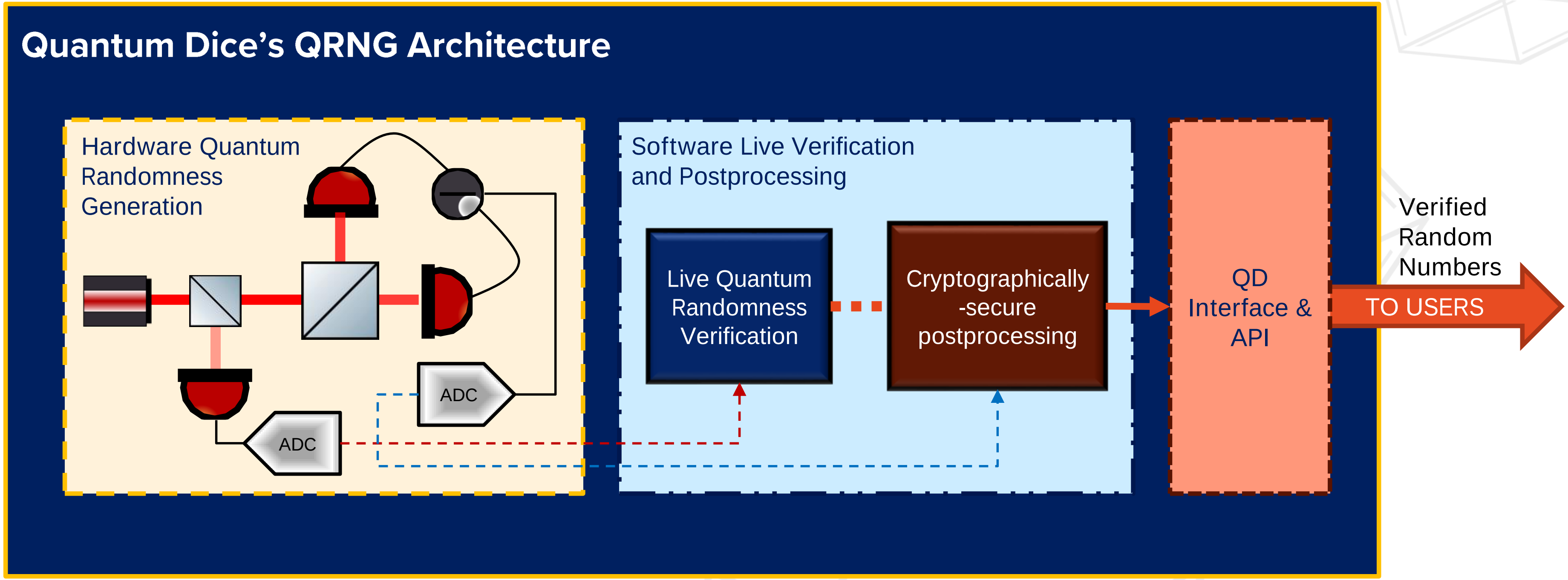
True Randomness.

# The Core Challenge

- Figuring out the entropy produced by simple idealized processes is easy
- Unfortunately, we cannot rely on flipping perfectly fair coins for the generation of our cryptographic keys in our security infrastructure
- Whether you are using classical hardware RNGs or are looking to use a quantum process, the challenge remains the same: how do you assess and. more importantly, guarantee the amount of randomness produced?

# Our Solution

SOURCE DEVICE INDEPENDENT SELF-CERTIFICATION (DISC™)



# Our Solution

## SOURCE DEVICE INDEPENDENT SELF-CERTIFICATION (**DISC**™)

Software Live Verification and Postprocessing

Hardware Quantum Entropy Generation


Secure Encryption Keys

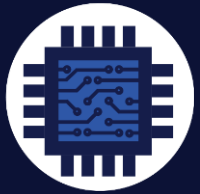
Patent: WO2018087516A1
DISC™ patent owned by the University of Oxford,
licensed Exclusively and Perpetually to Quantum Dice

QUANTUM DICE

# Our Solution

SOURCE DEVICE INDEPENDENT SELF-CERTIFICATION (DISC™)

Protects against attacks

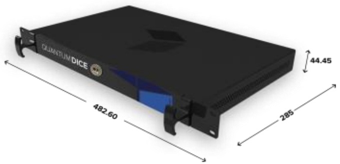


Enables integrated design

Prevents silent failure

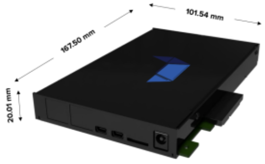
# Our Solution

## SOURCE DEVICE INDEPENDENT SELF-CERTIFICATION (**DISC**™)



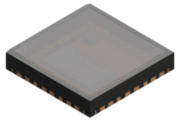

### APEX

- Rack-mount QRNG
- Generation Rate of up to 7.5 Gbps
- Suited for applications in data centres and enterprise hubs




### VERTEX

- PCIe QRNG
- Generation rate of up to 2.66 Gbps
- Suited for integration within networking and cybersecurity hardware

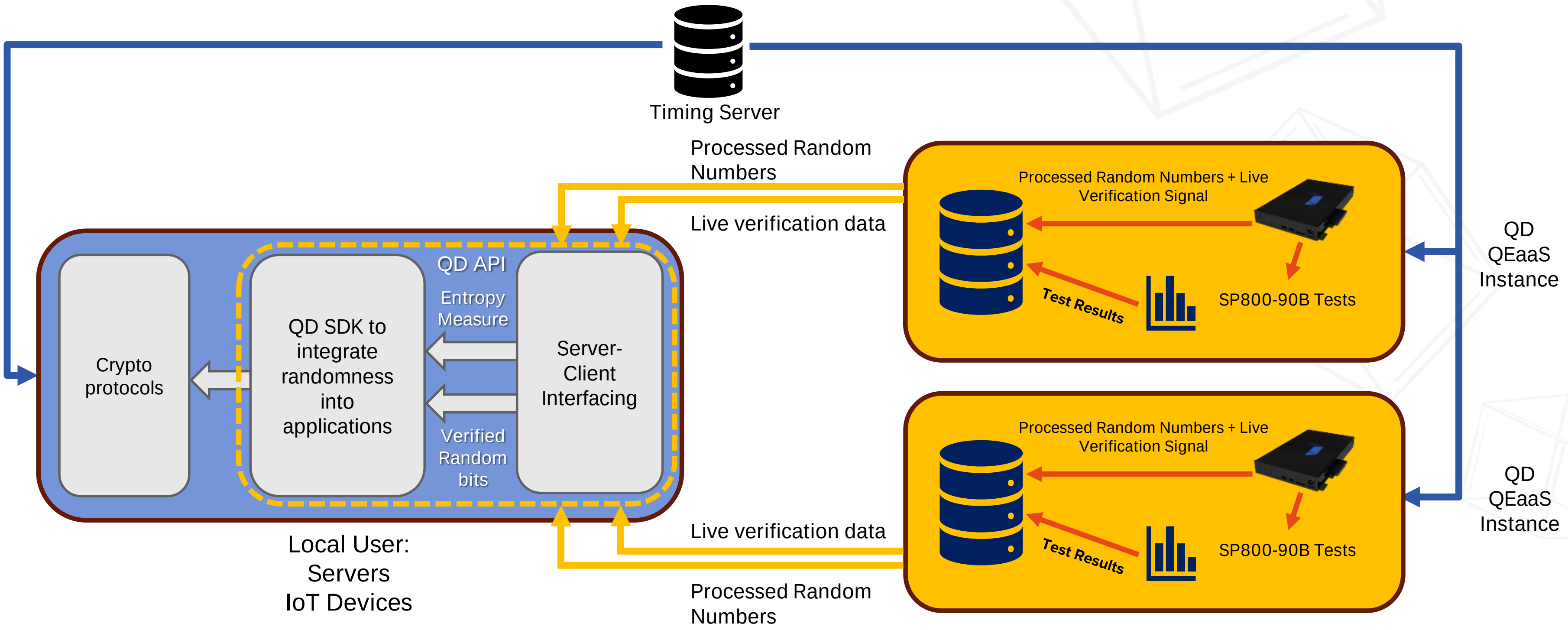


### Chip

- multi-GHz entropy source
- simple integration using standard electronic interfaces
- 5mm*5mm QFN Package

# Our Solution

SOURCE DEVICE INDEPENDENT SELF-CERTIFICATION (**DISC**™)



# Thank You.

annika.moslein@quantum-dice.com
george.dunlop@quantum-dice.com

QUANTUM DICE

Trust Nature.

# TAKE A MINUTE AND GIVE US FEEDBACK ...

RATE NOW!