WELCOME TO

Quantum Computing for Humans

Joseph Ellis, CISM, CRISC, CISSP, Security+
Boost Consulting Manager
CoNetrix Security

Tandem

DISCLAIMER

- **This presentation is for information only.**
  Evaluate risks before acting on ideas from this session.

- **This presentation contains opinions of the presenters.**
  Opinions may not reflect the opinions of Tandem.

- **This presentation is proprietary.**
  Unauthorized release of this information is prohibited.

Tandem

SESSION INFO

AUDIO/VIDEO

If you cannot hear sound or see the presentation now, adjust or change your settings.

SURVEY

At the end, fill out the survey for a chance to win an Amazon gift card.

RESOURCES

The slides, a recording, and certificate of attendance will be sent via email.

QUESTIONS

Use the “Questions” panel to chat with the presenters and Tandem team.

Tandem

- Audit Management
- Business Continuity Plan
- Compliance Management
- Cybersecurity
- Identity Theft Prevention
- Incident Management
- Internet Banking Security
- Phishing
- Policies
- Risk Assessment
- Vendor Management

Tandem™

A CoNetrix company

SUBMIT YOUR QUESTIONS!

Tandem

ABOUT THE PRESENTER

Joseph Ellis

Boost Consulting Manager

LinkedIn.com/in/josephellis-tx

Tandem

Agenda

- The Basics
- Security Considerations
- Take Action

POLL QUESTION

How interested in Quantum Computing are you?

Tandem

POLL QUESTION

How **FEARFUL** of Quantum Computing are you?

Tandem

Quantum Computing

"The sky is falling!"

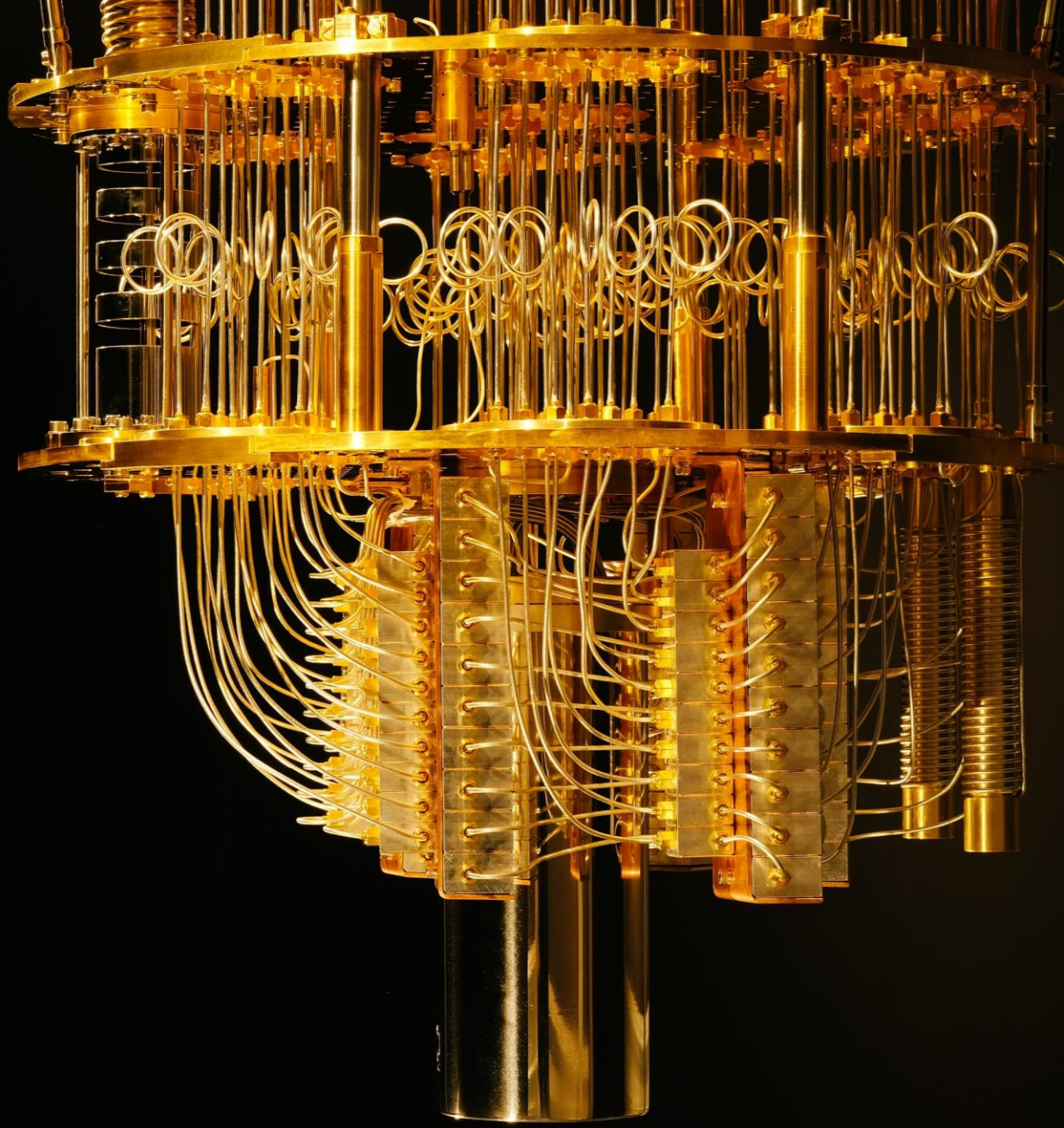
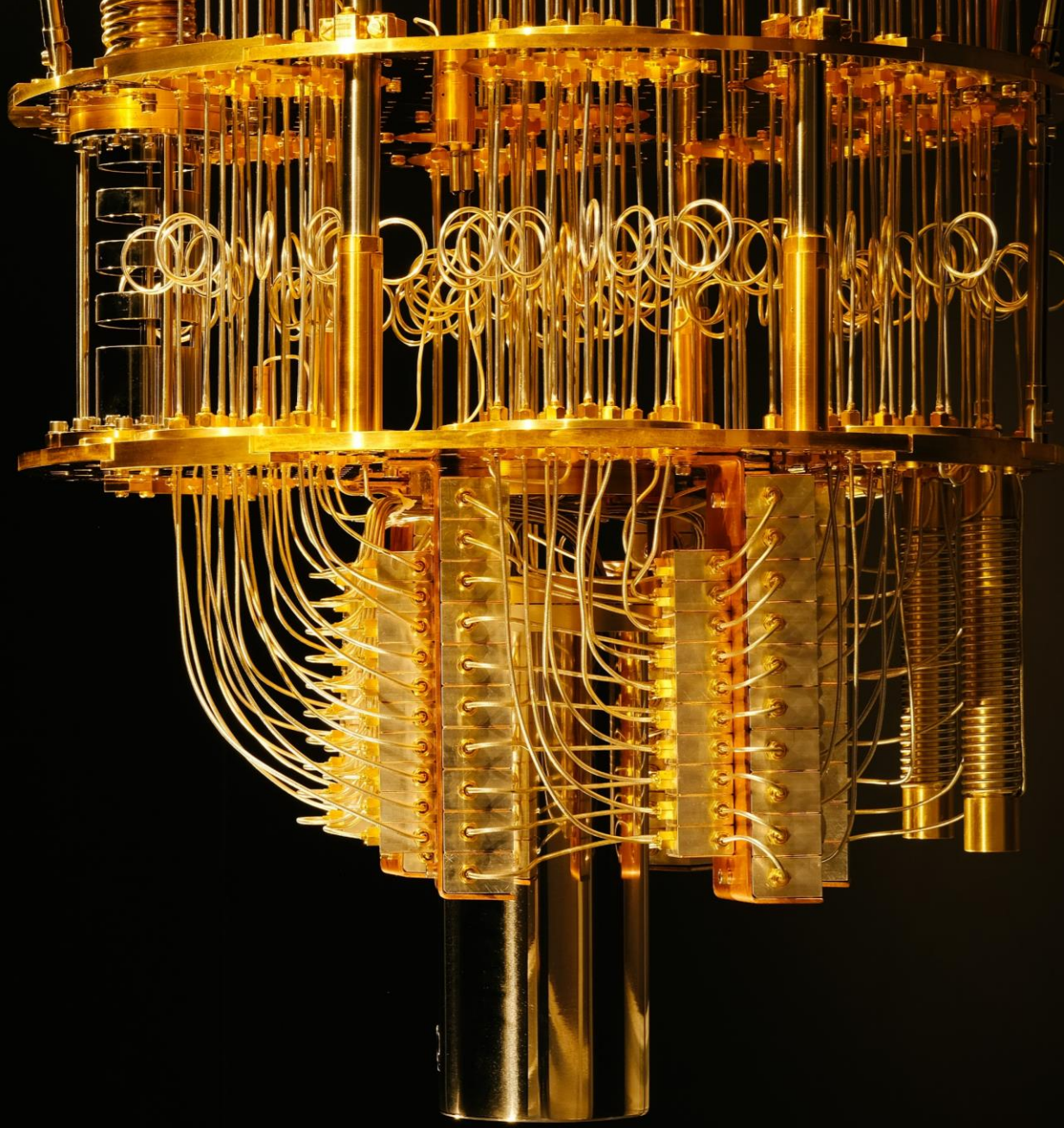


Image courtesy IBM Media Center

Quantum Computing

“There have already been examples of large batches of encrypted data being stolen by unknown actors, **possibly to be hoarded and decrypted later by using future technology**.

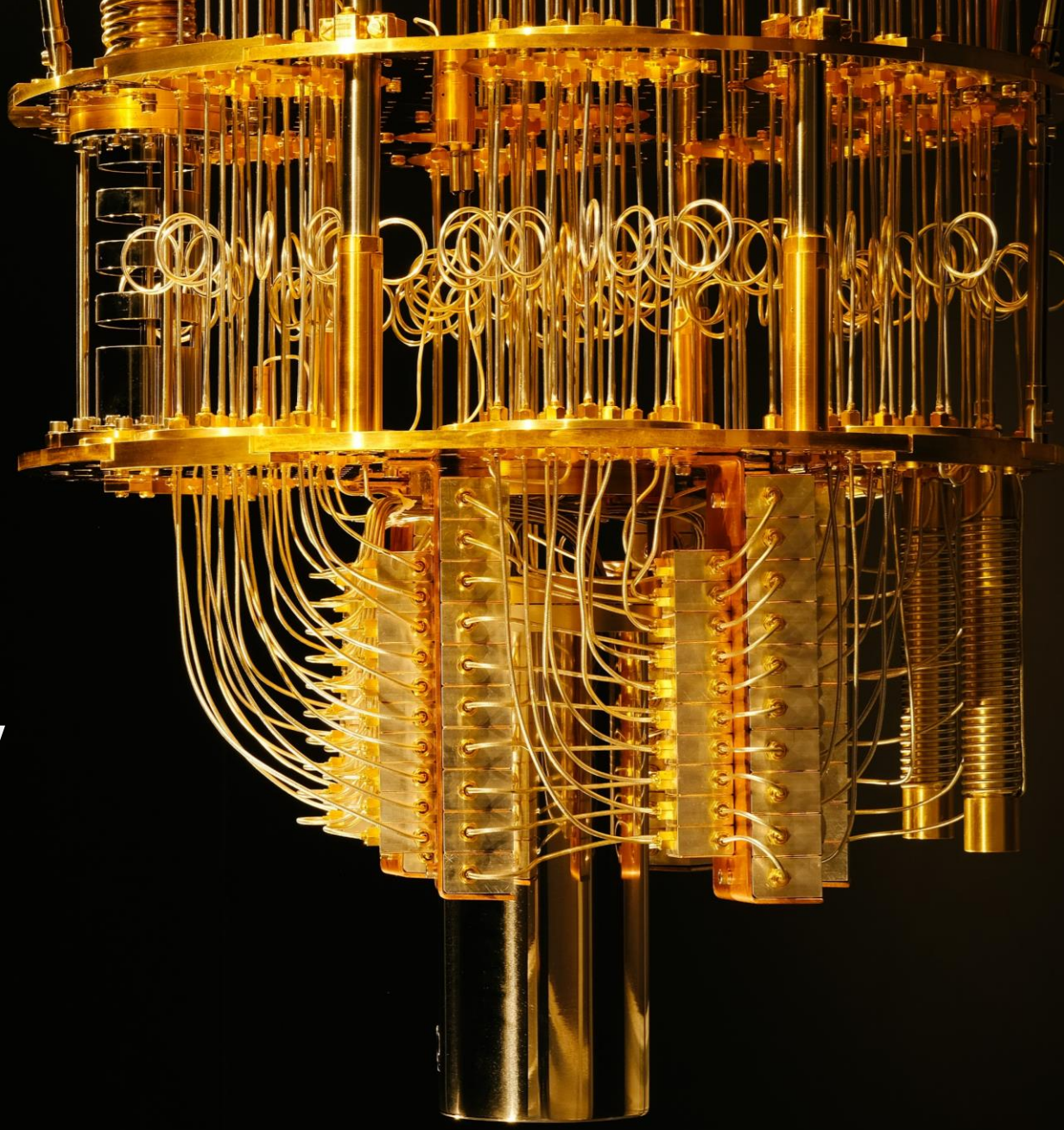


IBM, “What is quantum-safe cryptography?”
https://www.ibm.com/topics/quantum-safe-cryptography

Image courtesy IBM Media Center

Quantum Computing

“Not every data breach is discovered. **Any data not encrypted using quantum-safe standards today should be considered already lost.**

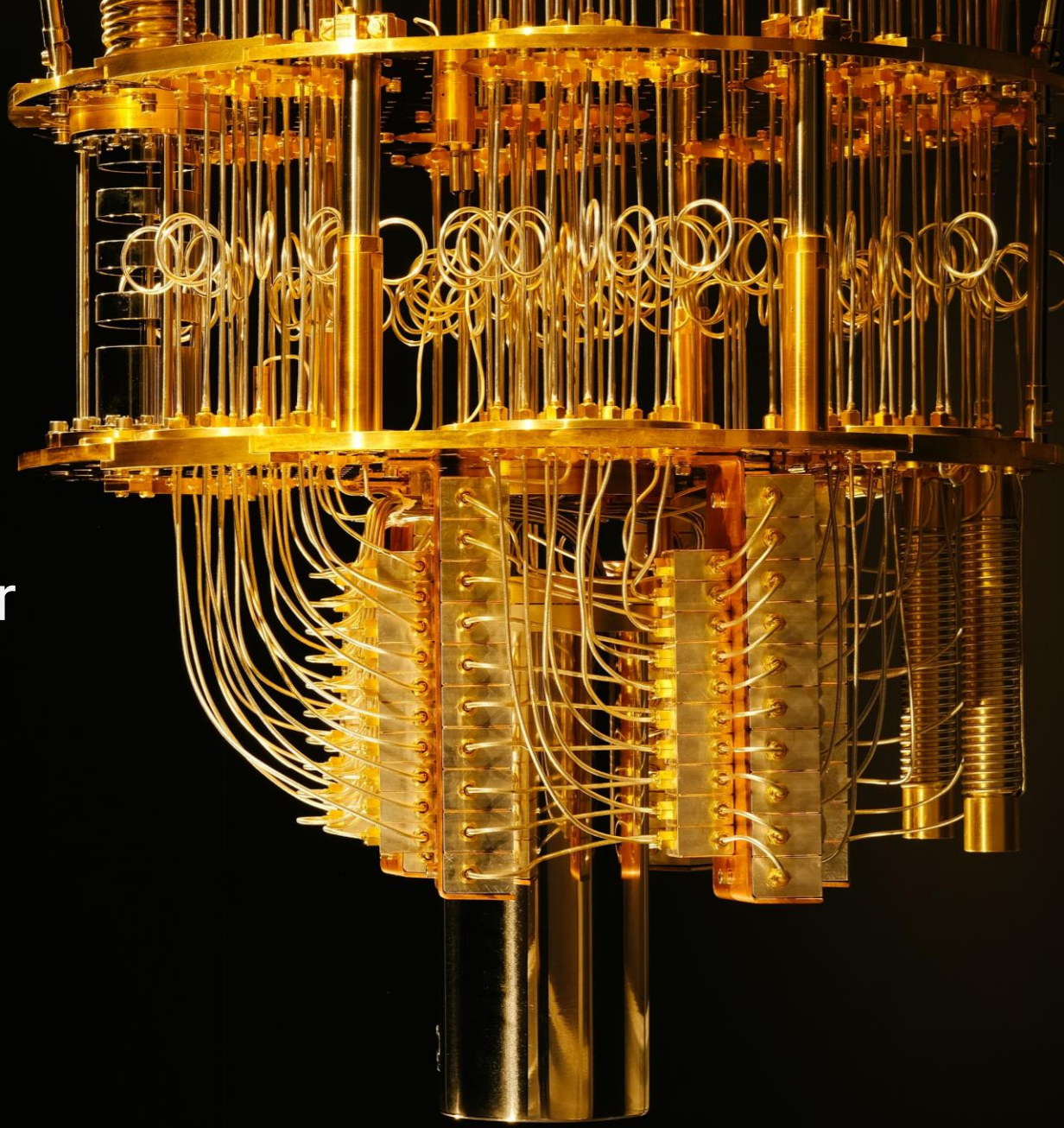


IBM, “What is quantum-safe cryptography?”
https://www.ibm.com/topics/quantum-safe-cryptography

Image courtesy IBM Media Center

Quantum Computing

“If you’re ready to act to protect your organization, the first step is to contact an IBM representative.”



IBM, “What is quantum-safe cryptography?”
https://www.ibm.com/topics/quantum-safe-cryptography

Image courtesy IBM Media Center

The Basics

Tandem

What is Quantum Computing, anyway?

Tandem

Coin Computing

Tandem

Coin Computing

Tandem

Coin Computing

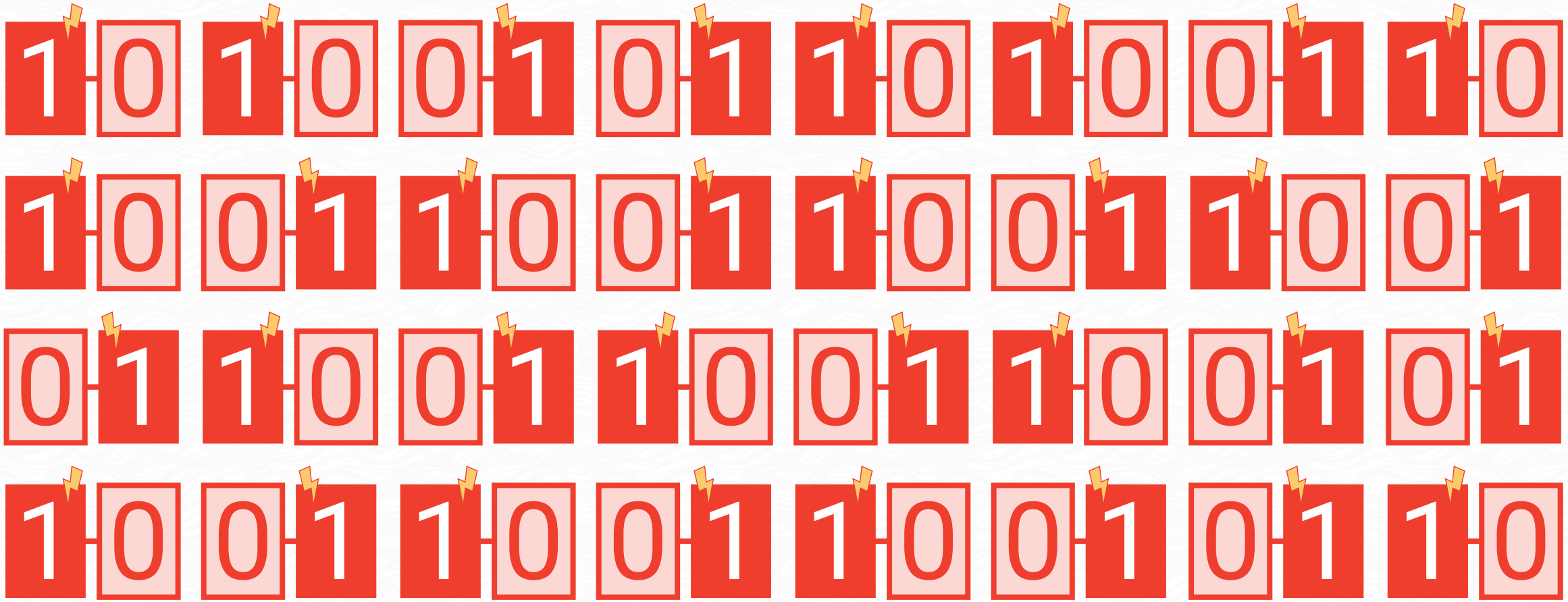
1 2 3 4

Tandem

Traditional Computing

Tandem

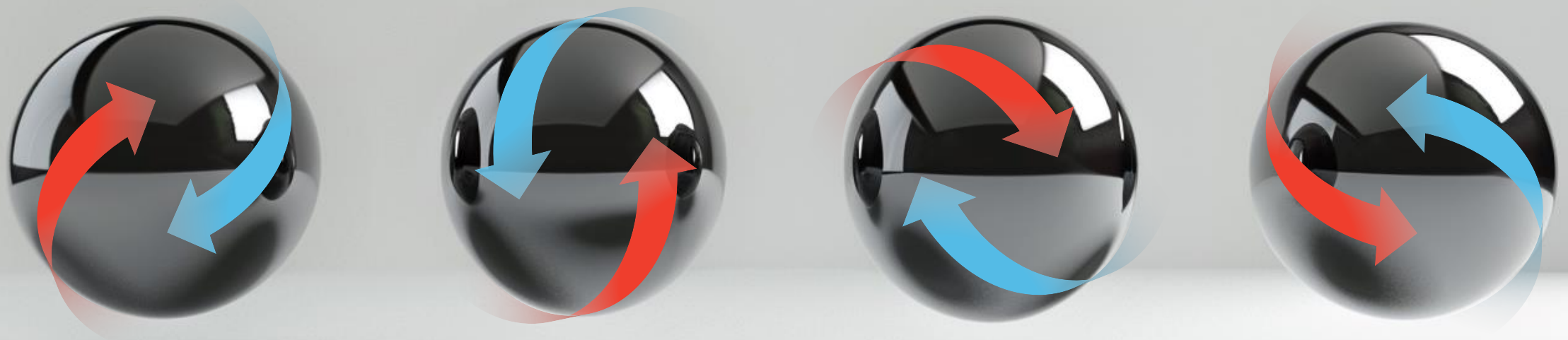
Traditional Computing



Tandem

QUANTUM COMPUTING

Quantum Computing



Qubits
Superposition

Tandem


Tandem

Security Considerations

Tandem

POLL QUESTION

How much would you say you **LOVE** math?

Tandem

Encryption

“Encryption uses math to protect sensitive electronic information, including the secure websites we surf and the emails we send.

Widely used public-key encryption systems, **which rely on math problems that even the fastest conventional computers find intractable**, ensure these websites and messages are inaccessible to unwelcome third parties.”

“NIST Announces First Four Quantum-Resistant Cryptographic Algorithms”, July 2022

Tandem


Tandem

Factoring

$21 = 7 \times 3$

$589 = 19 \times 31$

Tandem

Factoring

2271109657295089438126732046783160281980413790315184793946932235968178538976936789851159929183020345892030402942331837763843035866183250236826189427319820836291980285801873167460241766280380139266209769305593666500942338271388291899180812405278977640789143108340988718475071361723519196778237630975954714150 59

Factoring

3316168417829610832584679326283002267239813128404018693570786836250576270476624411258192895124897883591920703350613067254603426306342664766246120461395855650858224411887099209614313363676290624792607790927860566828981298749299969508553040397689724995835530632997521325585606060382581812010248092028823836832 13

Factoring

753695942276973745626235236679260610184276071133581436616824488723013945900685633138409796140400160907036377827331886910861072076652298594602328880052486042103060318338825644379032726927746980324377647865663078823314979657805621883127860713895116093641216891390381340751077225187673662339822716350372970182734447458232082365502827126339793721640164910036377352414057814749016711915694285292364 93

Factoring

22711096572950894381267
32046783160281980413790
31518479394693223596817
85389769367898511599291
83020345892030402942331
83776384303586618325023
68261894273198208362919
80285801873167460241766
28038013926620976930559
36665009423382713882918
99180812405278977640789
14310834098871847507136
17235191967782376309759
5471415059

x

33161684178296108325846
79326283002267239813128
40401869357078683625057
62704766244112581928951
24897883591920703350613
06725460342630634266476
62461204613958556508582
24411887099209614313363
67629062479260779092786
05668289812987492999695
08553040397689724995835
53063299752132558560606
03825818120102480920288
2383683213

=

75369594227697374562623
52366792606101842760711
33358143661682448872301
39459006856331384097961
40400160907036377827331
88691086107207665229859
46023288800524860421030
60318338825644379032726
92774698032437764786566
30788233149796578056218
83127860713895116093641
21689139038134075107722
51876736623398227163503
72970182734447458232082
36550282712633979372164
01649100363773524140578
14749016711915694285292
36493

Tandem

Factoring

"To give you an idea of the scale: **factoring a 500 digit number into its primes could take as long as the planet's formation**, and for huge numbers, the factoring process could take longer than the age of the universe itself."

Andreas Maier, "Prime numbers and their importance to modern life", CodeCoda, August 16, 2021, emphasis in the original

Tandem

Solutions and Strategies

Tandem

Quantum-Safe Cryptography

Quantum-resistant encryption algorithms:

CRYSTALS-Kyber
CRYSTALS-Dilithium
FALCON
SPHINCS+

“NIST Announces First Four Quantum-Resistant Cryptographic Algorithms”, July 2022

Tandem

Quantum-Safe Cryptography

First three finalized Post-Quantum Encryption Standards:
Federal Information Processing Standard (FIPS)

FIPS 203 (CRYSTALS-Kyber, renamed ML-KEM)
FIPS 204 (CRYSTALS-Dilithium, renamed ML-DSA)
FIPS 205 (Sphincs+, renamed SLH-DSA)

"NIST Releases First 3 Finalized Post-Quantum Encryption Standards", August 2024

Tandem

Quantum-Safe Cryptography

"We encourage system administrators to start integrating them into their systems immediately, because **full integration will take time**."

"There is no need to wait for future standards. Go ahead and start using these three."

"NIST Releases First 3 Finalized Post-Quantum Encryption Standards", August 2024

Tandem

Guidance!

1. **Establish a quantum-readiness roadmap.**

   [Establish] a project management team to plan and scope the organization's migration to PQC. Quantum-readiness project teams should initiate proactive cryptographic discovery activities that **identify the organization's current reliance on quantum-vulnerable cryptography**.

Quantum-Readiness: Migration to Post-Quantum Cryptography, August 2023

Tandem

Guidance!

2. Prepare a cryptographic inventory.

Organizations should create a cryptographic inventory that offers **visibility into how the organization leverages cryptography** in its IT and OT systems.

Quantum-Readiness: Migration to Post-Quantum Cryptography, August 2023

Tandem

Guidance!

3. **Discuss post-quantum roadmaps with technology vendors.**

   [Engage with] technology vendors to learn about vendors' quantum-readiness roadmaps, including migration.

   Solidly built roadmaps should describe how vendors plan to migrate to PQC, charting timelines for testing PQC algorithms and integration into products.

Quantum-Readiness: Migration to Post-Quantum Cryptography, August 2023

Tandem

Guidance!

4. Supply chain quantum-readiness:

Organizations should develop an understanding of their reliance/dependencies on quantum-vulnerable cryptography in systems and assets, as well as **how the vendors in their supply chain will be migrating to PQC.**

Quantum-Readiness: Migration to Post-Quantum Cryptography, August 2023

Tandem


Questions?
Tandem

Fill out the survey for a chance to win!

Tandem

- Audit Management
- Business Continuity Plan
- Compliance Management
- Cybersecurity
- Identity Theft Prevention
- Incident Management
- Internet Banking Security
- Phishing
- Policies
- Risk Assessment
- Vendor Management

Tandem™

A CoNetrix company

Virtual Information Security Officer (VISO)

Consulting Retainer Services

Risk Assessment Services

Business Continuity Planning

Information Security Policies Services

Vendor Management

Cybersecurity Services

Audit Management

Incident Management

Consulting Workshops for Tandem

BOOST consulting™

by CoNetrix Security

Tandem


Questions?
Tandem

THANKS FOR JOINING

Quantum Computing for Humans

Joseph Ellis, CISM, CRISC, CISSP, Security+
jellis@conetrix.com
LinkedIn.com/in/josephellis-tx

Remember to complete the survey!

Tandem