

POST-QUANTUM PANIC: WHEN WILL THE CRACKING BEGIN, AND CAN WE DETECT IT?

KONSTANTINOS KARAGIANNIS **@KONSTANTHACKER**

DIRECTOR, QUANTUM COMPUTING SERVICES

PROTIVITI

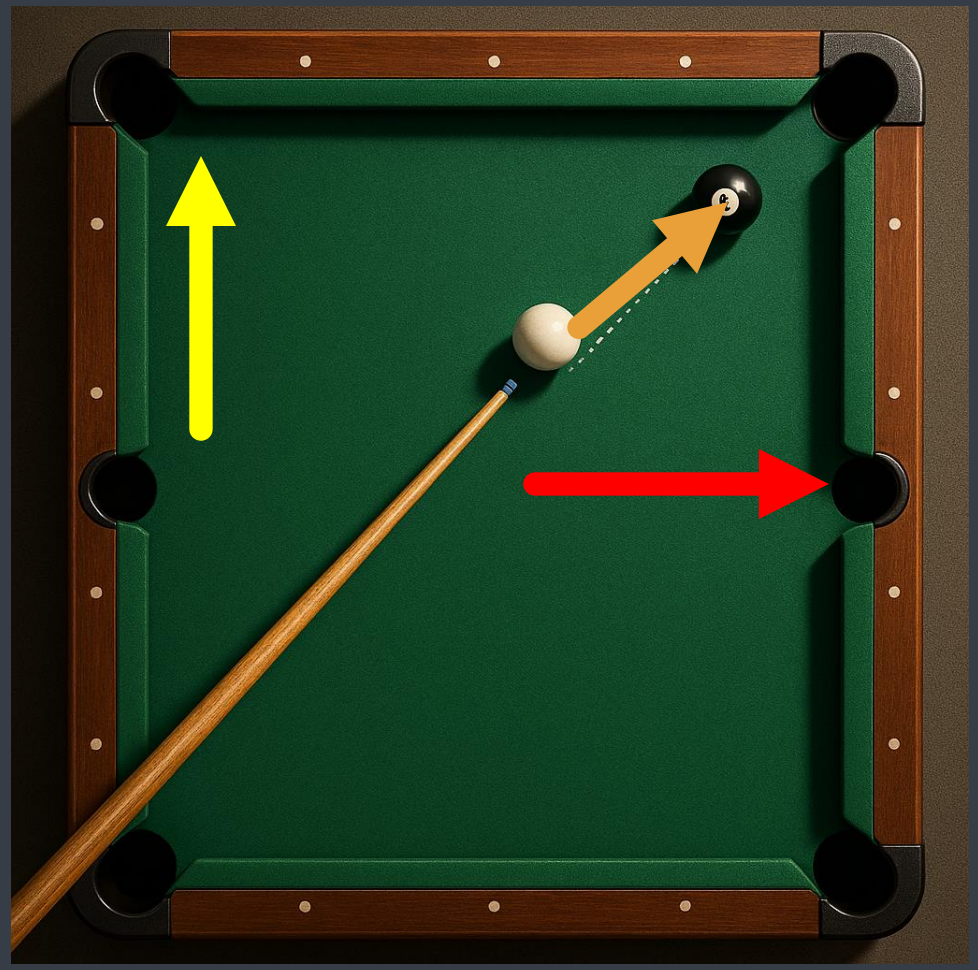
© 2025 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.

protiviti®


THE
POST-QUANTUM
WORLD
powered by protiviti®

QUANTUM: A TOPIC WORTHY OF A VILLAGE

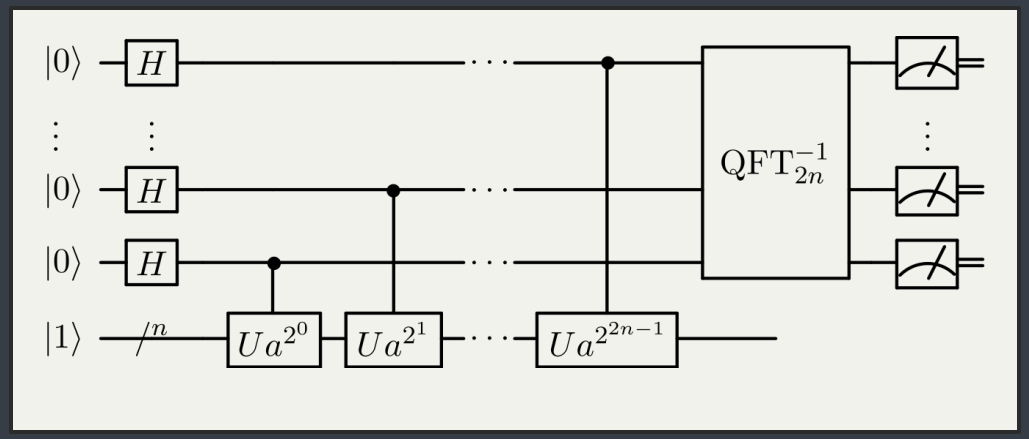
- What quantum is
- What it can do
- What it is not
- What it does not do!



protiviti®

THREATS TO CRYPTOGRAPHY

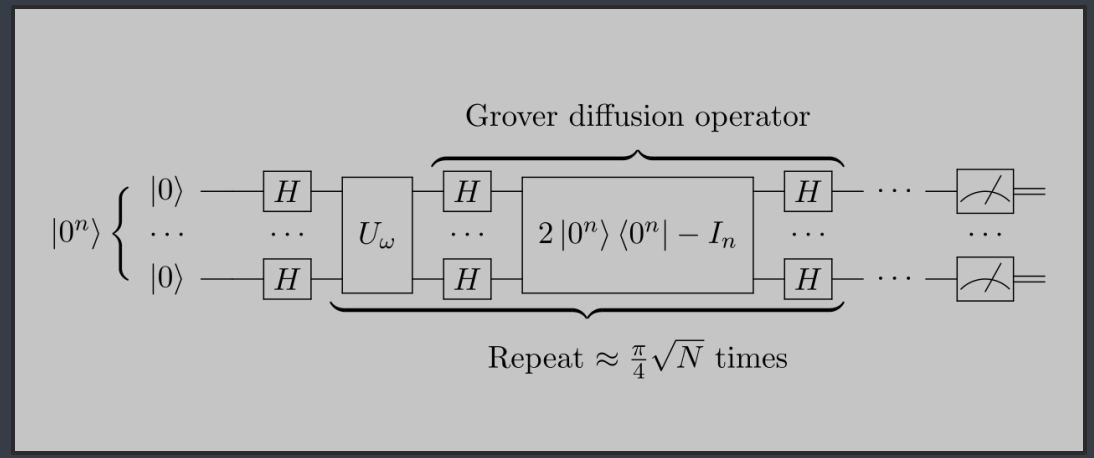
Public Key/Asymmetric



Factoring—Shor's 1994

Optimistic 2n+2 paper: https://arxiv.org/abs/1611.07995

Symmetric



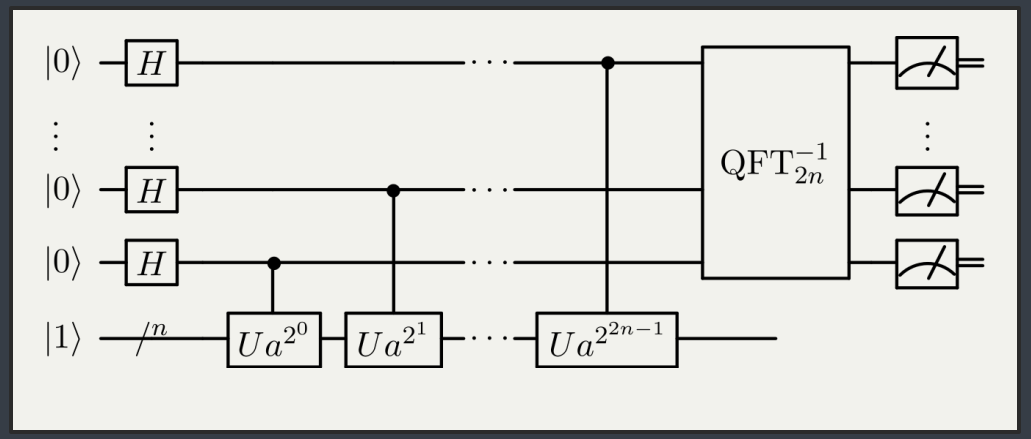
Brute-Force Search—Grover's 1996

2953 qubits AES 128: https://arxiv.org/abs/1512.04965

protiviti

THREATS TO CRYPTOGRAPHY





ECC

Under 2500: https://arxiv.org/abs/1706.06752

protiviti®

2035 IS Q-DAY … ACCORDING TO NIST

2024

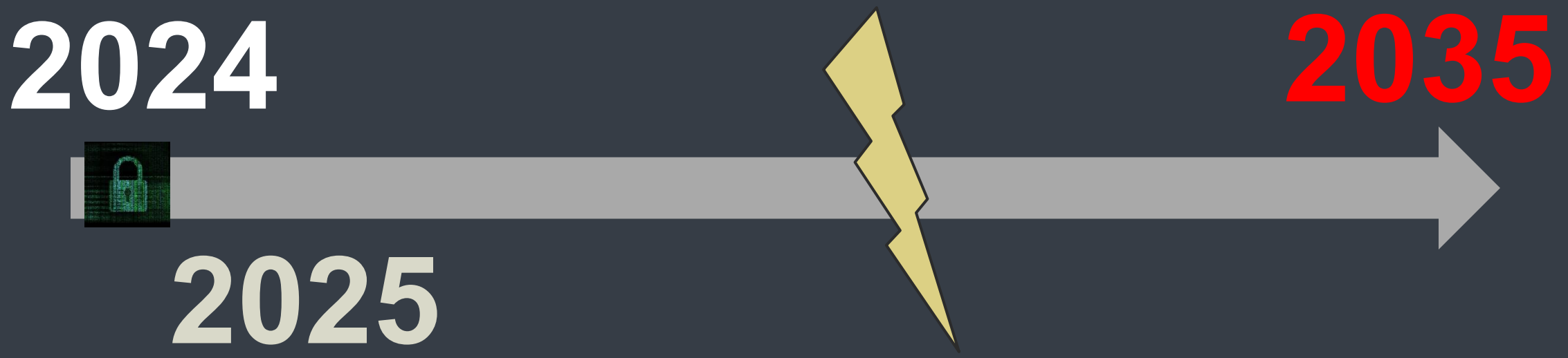


2025

2035

protiviti®

WHAT HAPPENS IF WE'RE WAY OFF?



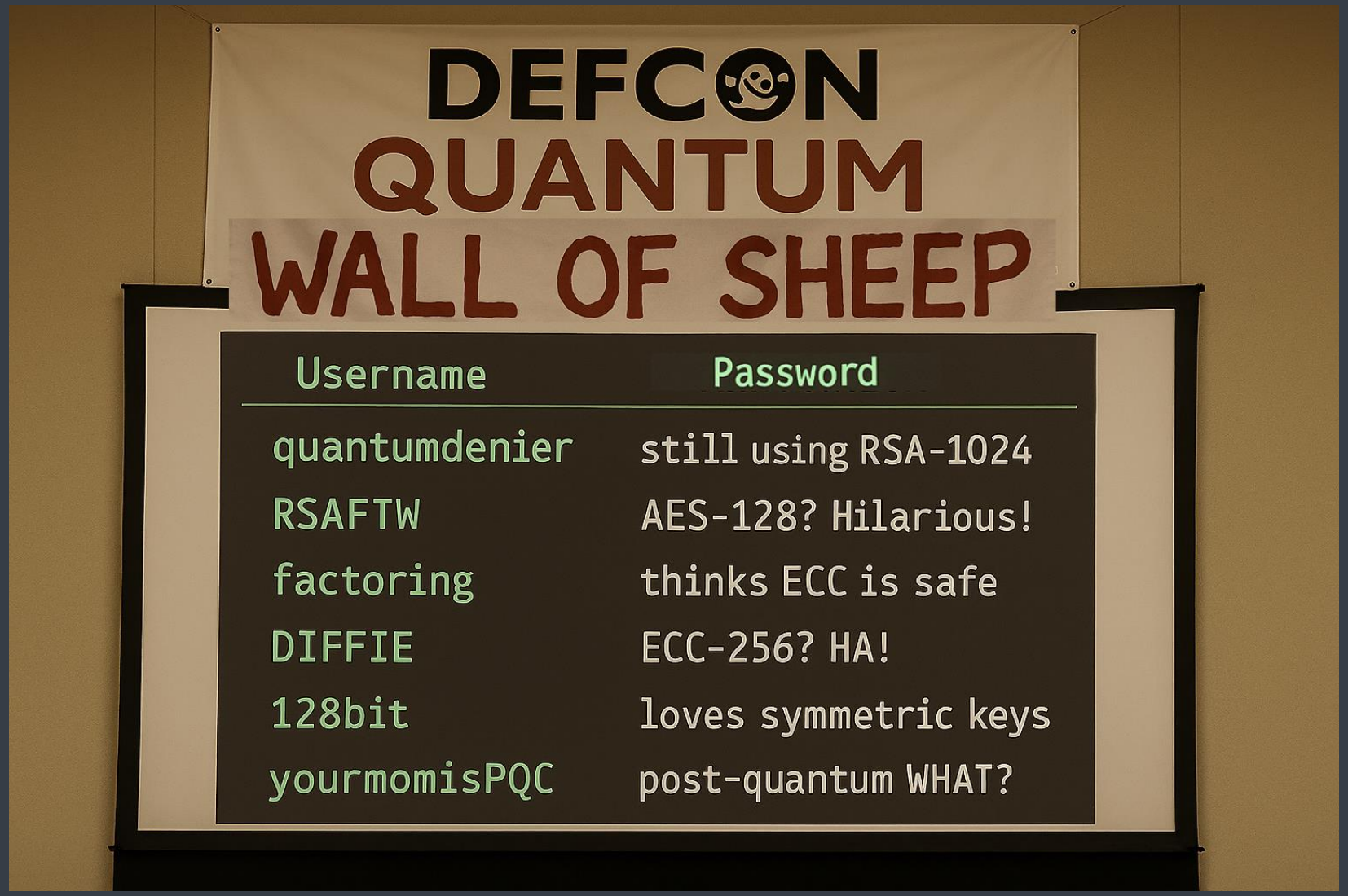
protiviti®

IMAGINE YEARS OR EVEN JUST MONTHS



protiviti®

HECK, IMAGINE 5 YEARS OF THIS



SHOR BASICS

- Classical Setup
- Quantum Period Finding
- Classical Post-Processing
- Some estimates: a billion noisy qubits

$$a^x \pmod N$$

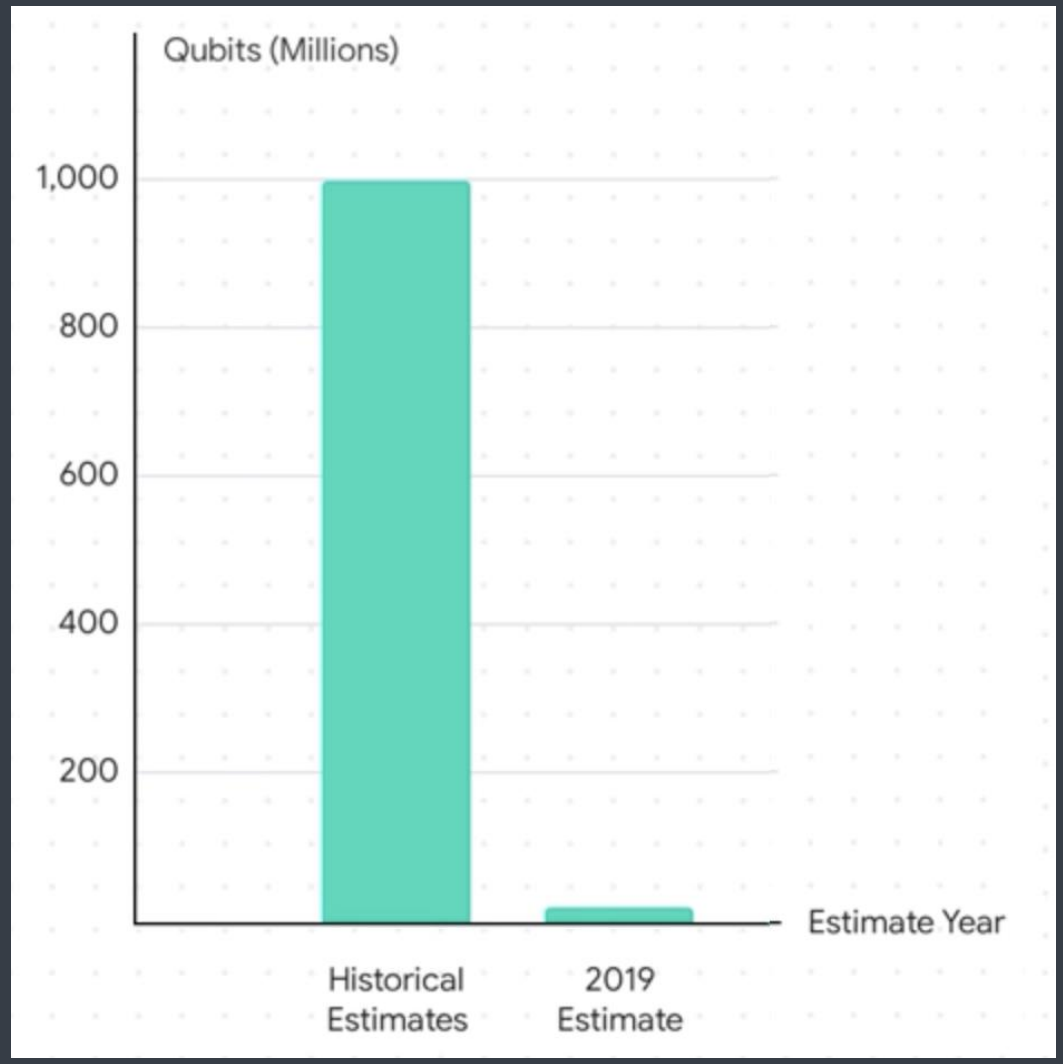
For a=4 and N=21:
$4^1 \rightarrow 4$, $4^2 \rightarrow 16$, $4^3 \rightarrow 1$, $4^4 \rightarrow 4$, $4^5 \rightarrow 16$, $4^6 \rightarrow 1$, ...

The pattern is 4,16,1 and its length (the period, r) is 3

GIDNEY & EKERÅ

- Optimized modular exponentiation
- 3n logical qubits/20 million physical

2019 (2021 final pub date)
https://arxiv.org/abs/1905.09749

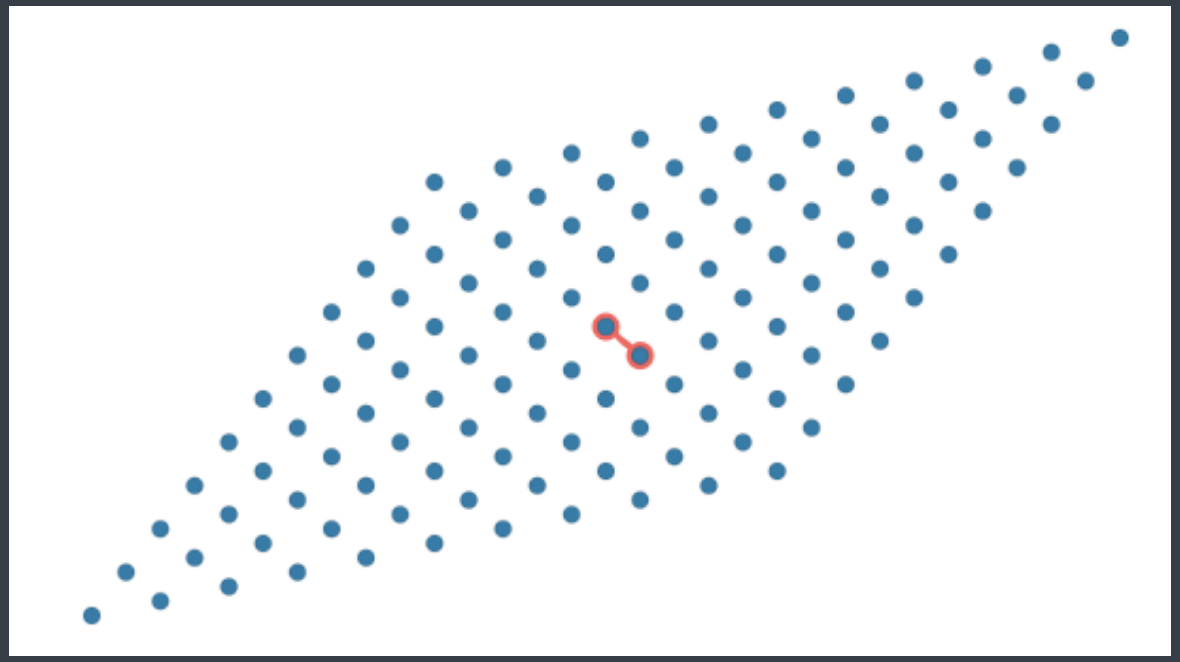


protiviti®

REGEV

- Reducing gate count
- Construct a Lattice and Sample
- Classical Post-Processing of small jobs

2023-24
https://arxiv.org/abs/2308.06572



protiviti

GIDNEY

- Reduce Logical Qubit Count
- Optimize Error Correction
- Trade Time for Space

2025
https://arxiv.org/abs/2505.15917

n	s	ℓ	w_1	w_3	w_4	f	m	P_{deviant}	E(shots)	Toffolis	Qubits
1024	8	18	6	3	6	28	640	2.87%	9.4	1.1e+09	742
1536	8	21	6	3	5	31	960	1.83%	9.3	3.1e+09	1074
2048	8	21	6	3	5	33	1280	1.25%	9.2	6.5e+09	1399
3072	8	21	6	3	5	35	1920	0.91%	9.2	1.9e+10	2043
4096	8	24	6	3	5	36	2560	0.80%	9.2	4.0e+10	2692
6144	8	24	6	3	5	39	3840	0.42%	9.1	1.2e+11	3978
8192	8	24	6	3	5	40	5120	0.40%	9.1	2.7e+11	5261

FACTORING QUBIT ESTIMATES

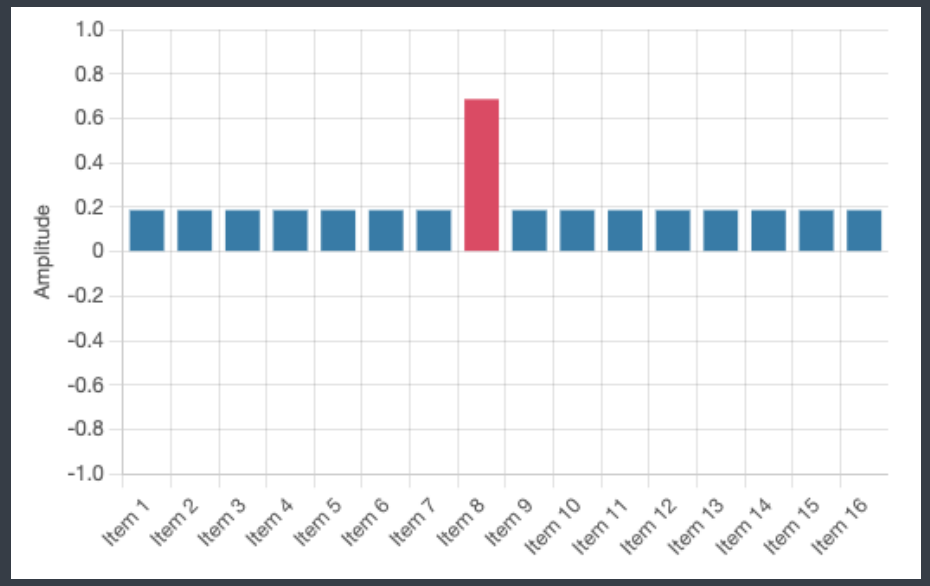
Method	Physical/Logical Qubits 2048-bit n	Estimated Runtime
Gidney & Ekerå (2021)	~20 million noisy/~6000	~8 hours (gates proportional to n^2)
Oded Regev (2024)	TBD/TBD (may not offer improvement at 2048 bits, only at higher scales)	TBD (faster than Shor, gates proportional to $n^{1.5}$)
Craig Gidney (2025)	<1 million noisy (~897,864)/~1400	<1 week (~5 days; trades Shor speed for 20x reduction in physical qubits)

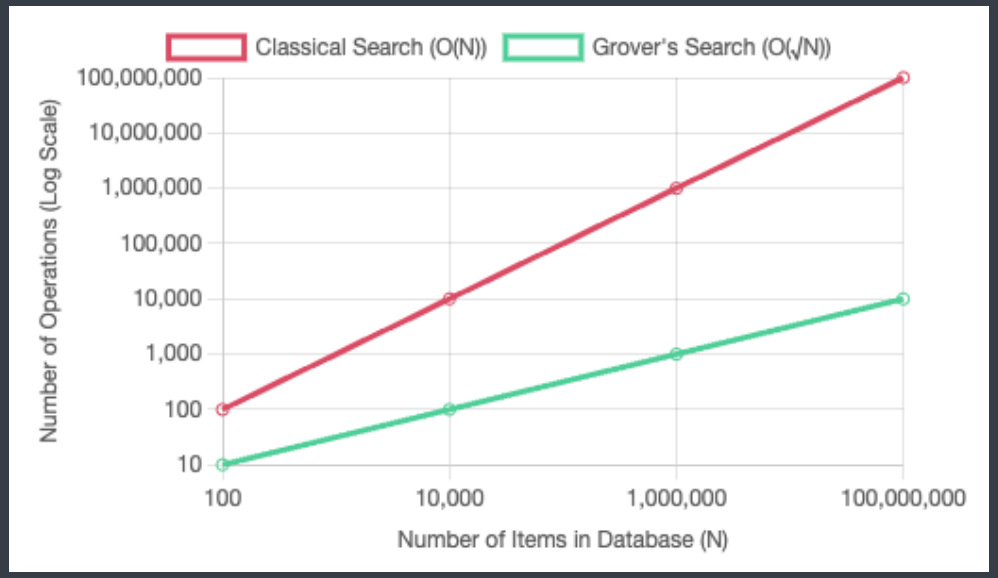
protiviti®

GROVER'S ALGORITHM

- Prepare Equal Superposition
- The Grover Loop
- Measure the System

Optimistic ~1000 for AES 128 https://arxiv.org/pdf/1512.04965

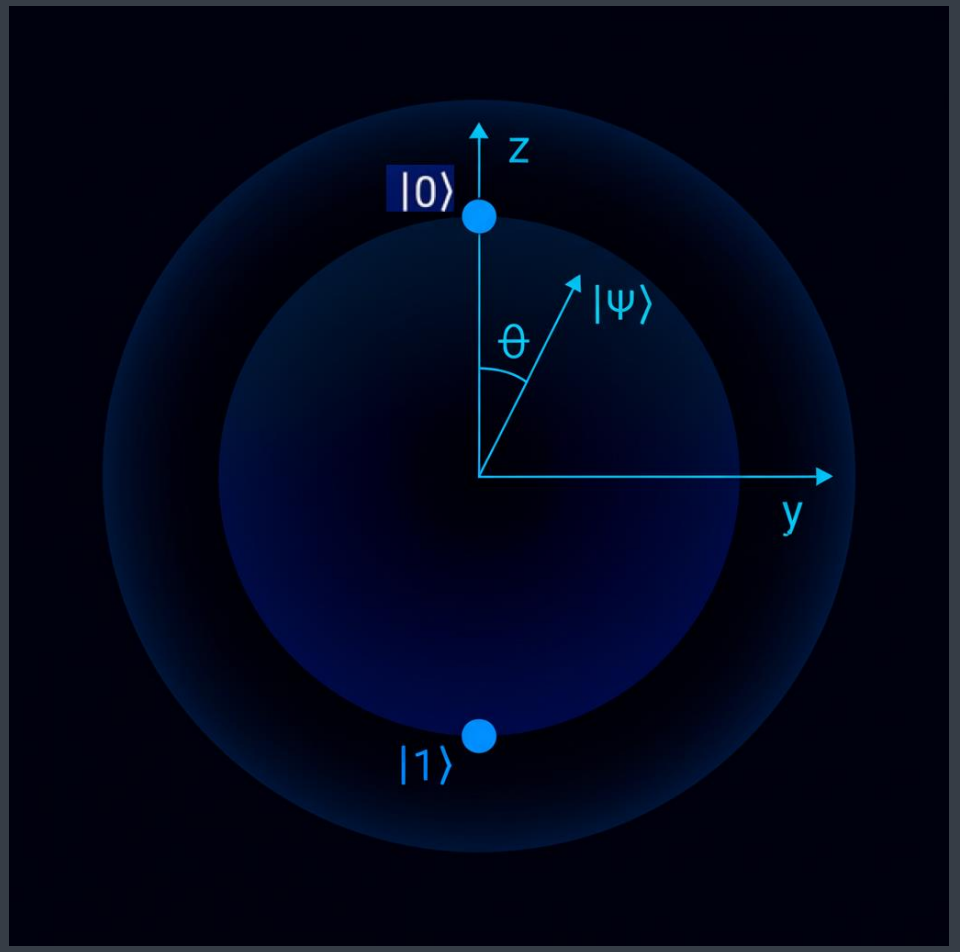




protiviti®

SO, REMEMBER THE OPTIMISTIC RANGES

- 1,400 TO 6,000 LOGICAL RSA 2048
- 1,000 TO 3,000 LOGICAL GROVER AES 128
- THESE MIGHT EVEN IMPROVE FURTHER…



protiviti®

AN AI SURPRISE?

AlphaEvolve: A Gemini-powered coding agent for designing advanced algorithms

14 MAY 2025

By AlphaEvolve team

Share



protiviti

BUT YEAH, REMEMBER THE OPTIMISTIC RANGES

- 1,400 TO 6,000 LOGICAL RSA 2048
- 1,000 TO 3,000 LOGICAL GROVER AES 128

protiviti®

IONQ TIMELINE

Updated Technology Roadmap

IONQ

	2025	2026	2027	2028	2029	2030
~~#AQ~~	~~64~~	~~256~~	~~384~~	~~1,024~~		
Qubits	64	256	10,000	20,000	200,000	2,000,000
Logical Qubits		12	800	1,600	8,000	80,000
Logical Error Rate		<1.00E-7			<1.00E-12	

protiviti

NO ONE HAS EVER DONE THIS

QUANTUM INSIDER
powered by RESONANCE

News Resources Product Advisory Marketing About Us

Chinese Scientists Report Using Quantum Computer To Hack Military-Grade Encryption

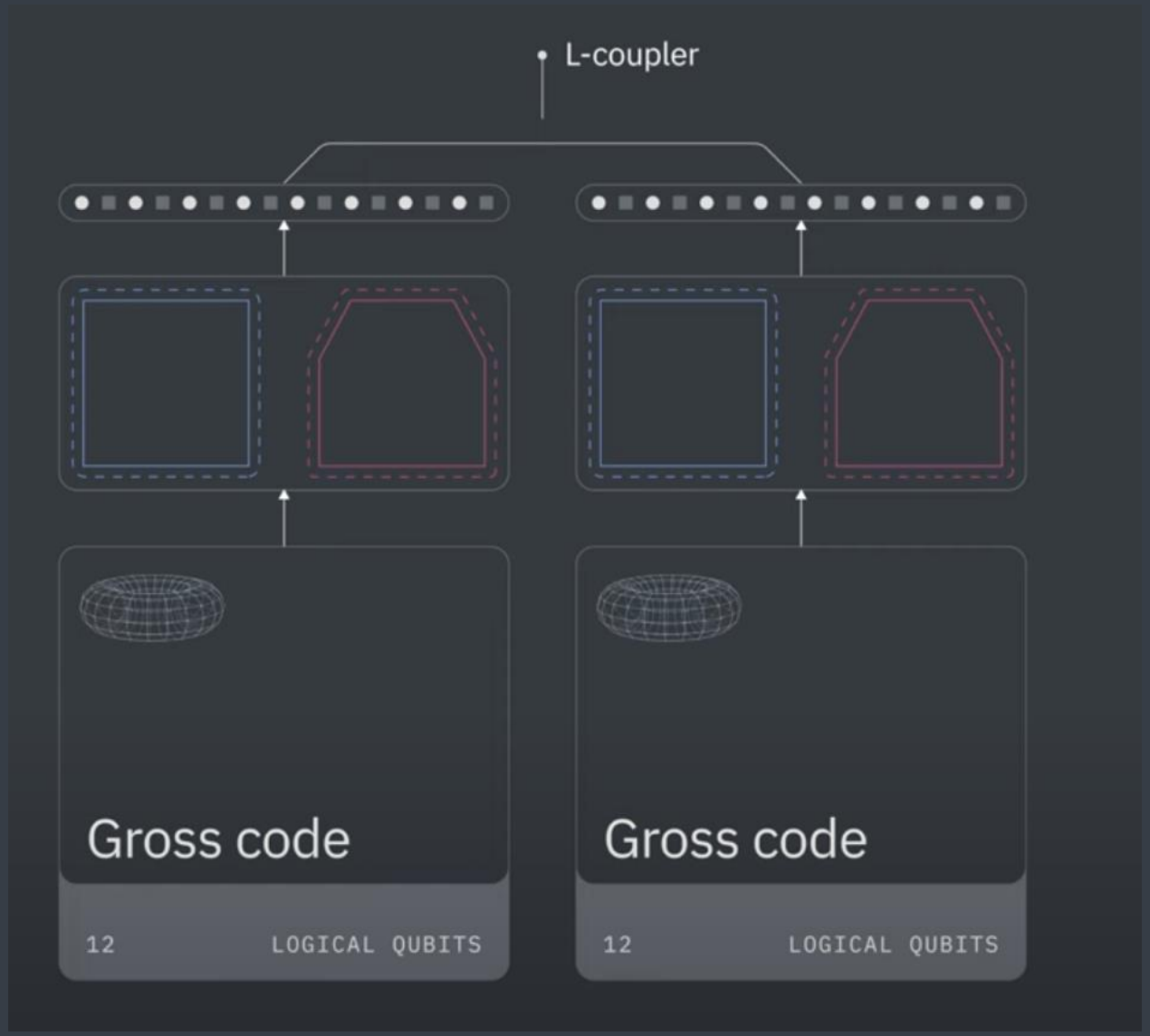
National, Quantum Computing Business, Reports, Research

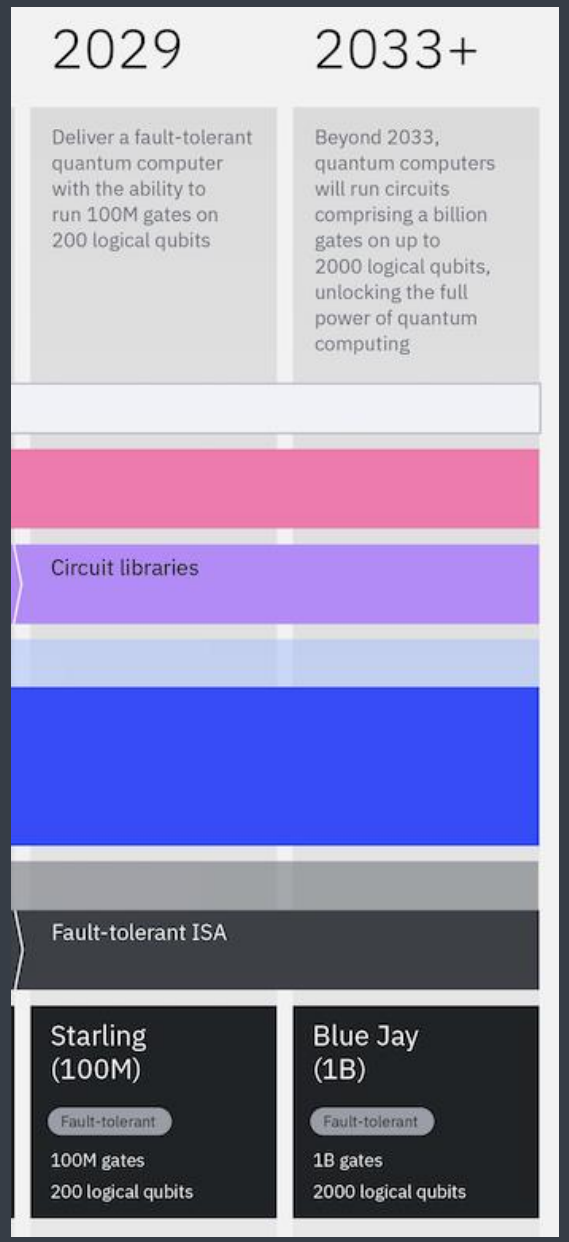
Matt Swayne • May 9, 2025



protiviti®

IBM TIMELINE





protiviti®

USE CASE EXAMPLES FOR FINANCE



Optimization

Portfolio Optimization

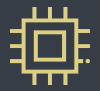
Optimal Trading Execution

Capital Allocation

Asset Liability Management

Transaction Settlement

Yield Curve Fitting



Machine learning

Credit Scoring

Default Early Warnings

Fraud Detection/AML

Predictive Analytics / Next Best Action



Pricing & simulation

Monte Carlo Simulations

Valuation & Regulatory Ratios

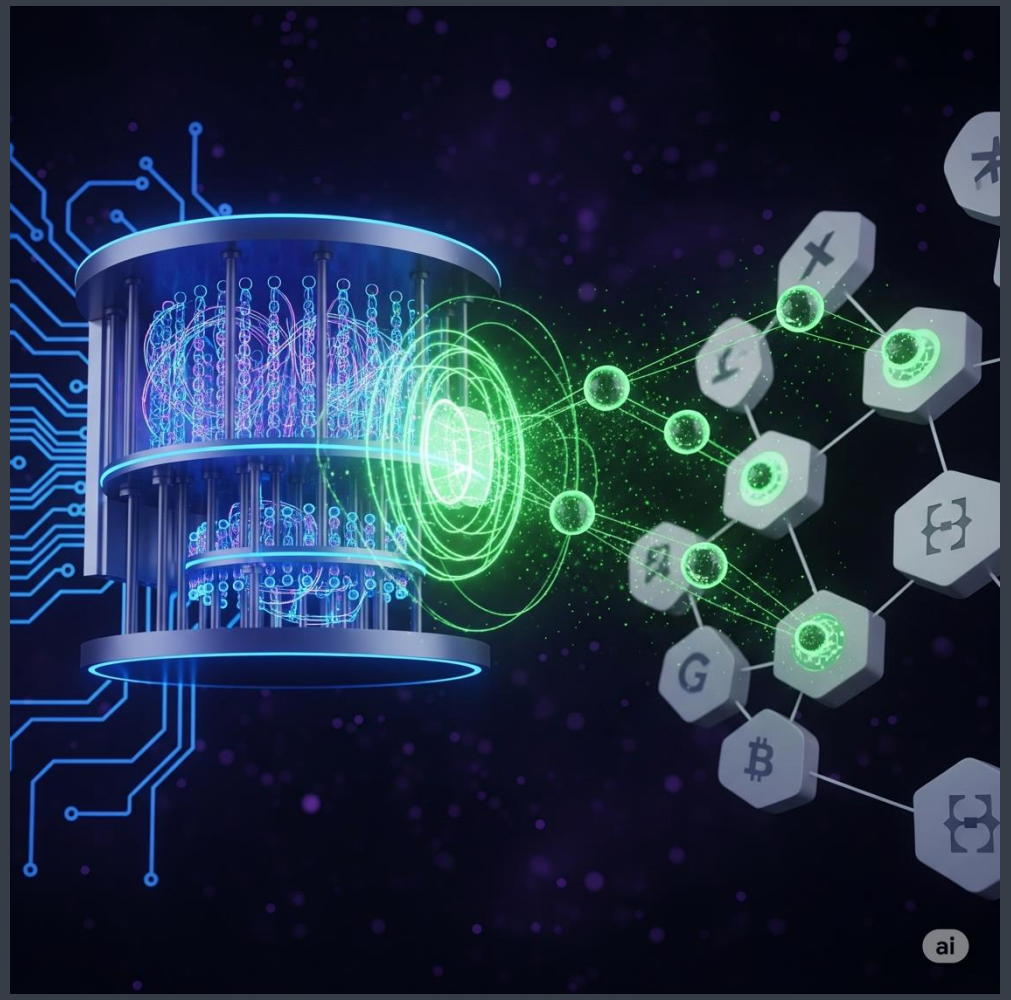
Options Pricing

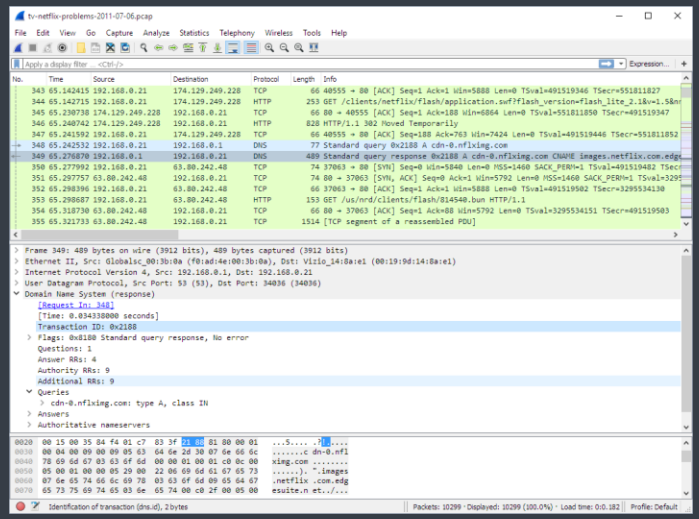
Risk Assessment & Tail Risk Simulations

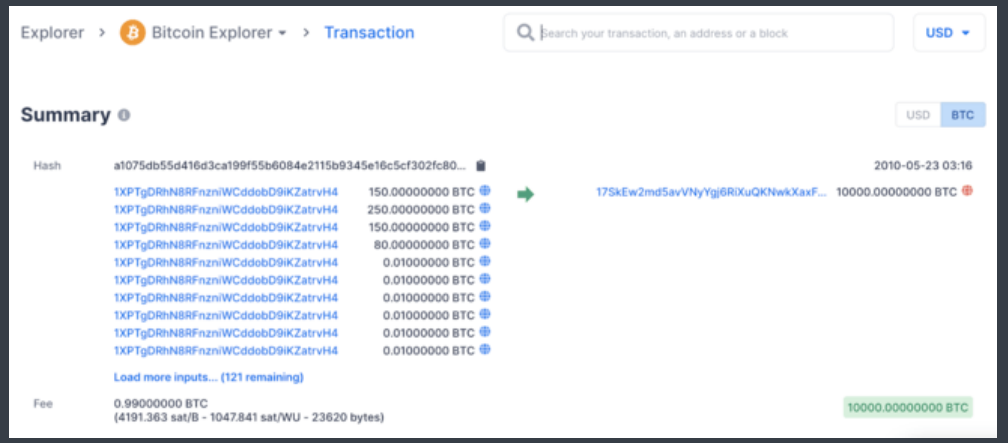
Multi-Factor Interest Rate Models

protiviti®

DETECTING ATTACKS LOCALLY?







protiviti®

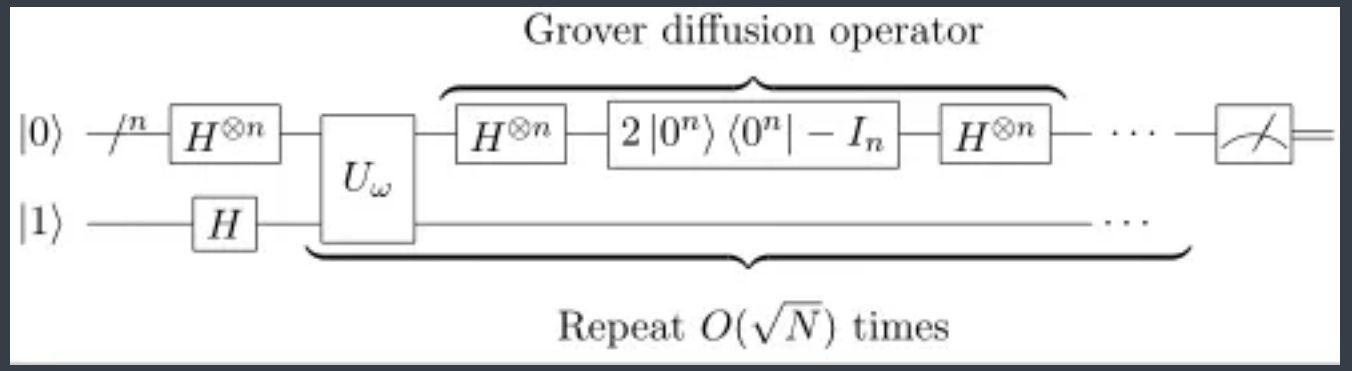
POINTS OF DETECTION ON THE STACK

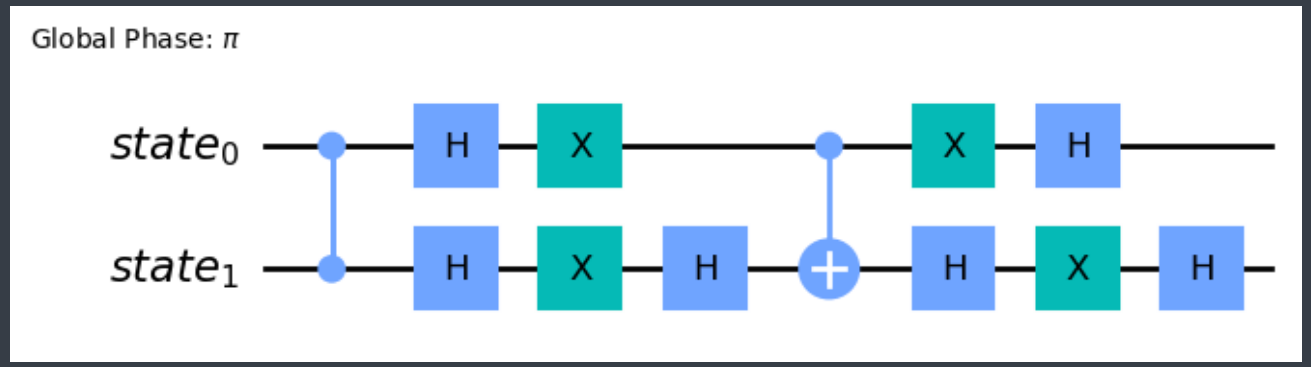
Algorithm	Patterns
Shor	Quantum Fourier Transform (QFT), modular exponentiation
Grover	Repeatedly applies two main blocks: oracle and the diffusion operator.

Note: And potentially crazy long runtimes!

1. **Code and Circuit Level (Software)**
2. **Compiler and Transpiler Level**
3. **Pulse Control Level (Hardware Interface)**
4. **Resource Utilization Metadata (Cloud Management)**

DETECTING GROVER RUNNING ON CLOUD





https://github.com/Qiskit/qiskit-tutorials/blob/master/tutorials/algorithms/06_grover.ipynb

protiviti

BUT WILL THEY? AN EXAMPLE



"If you use Amazon Braket to access quantum computers, your circuit and associated metadata will be sent to and processed by the hardware providers outside of facilities operated by AWS. Your content is anonymized so that only content necessary to process the quantum task is sent to the quantum hardware providers. AWS account information is not transmitted to them. All data is encrypted at rest and in transit, and is only decrypted for processing. In addition, Amazon Braket hardware providers are not permitted to store or use your content for purposes other than processing your task. "

"IonQ processes Customer End User Communications under the instructions of the relevant Customer, which is the "data controller" (or occupies a similar role as defined in applicable privacy laws), as described in the applicable Services Agreement between such Customer and IonQ. IonQ's obligations as a "data processor" or "service provider" with respect to such information are defined in such Services Agreement and applicable data protection addendum and are not made part of this Privacy Policy."



protiviti

WHO WILL BE DOING THE CRACKING?



protiviti®

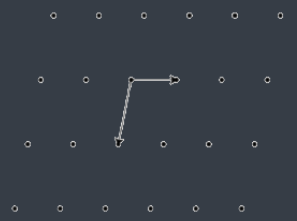
TYPES OF TARGETS, NOW AND THEN

X + Y > Z ?

protiviti®

TYPES OF PQC

Lattice-Based Cryptography



Hash-Based Signatures

#

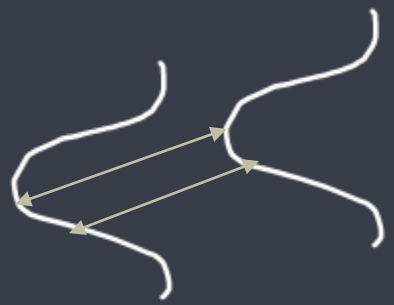
Code-Based Cryptography

01001001010010 0

Multivariate Cryptography

$$x^2 + y^2 + z^2$$

Isogeny-Based Cryptography



protiviti®

FIRST NIST PQC STANDARDS

Public Key Encryption/KEM

ML-KEM

Module-Lattice-Based Key-Encapsulation Mechanism Standard

(Formerly CRYSTALS-Kyber) FIPS 203

Digital Signatures

ML-DSA

Module-Lattice-Based Digital Signature Standard

(Formerly CRYSTALS-Dilithium) FIPS 204

SLH-DSA

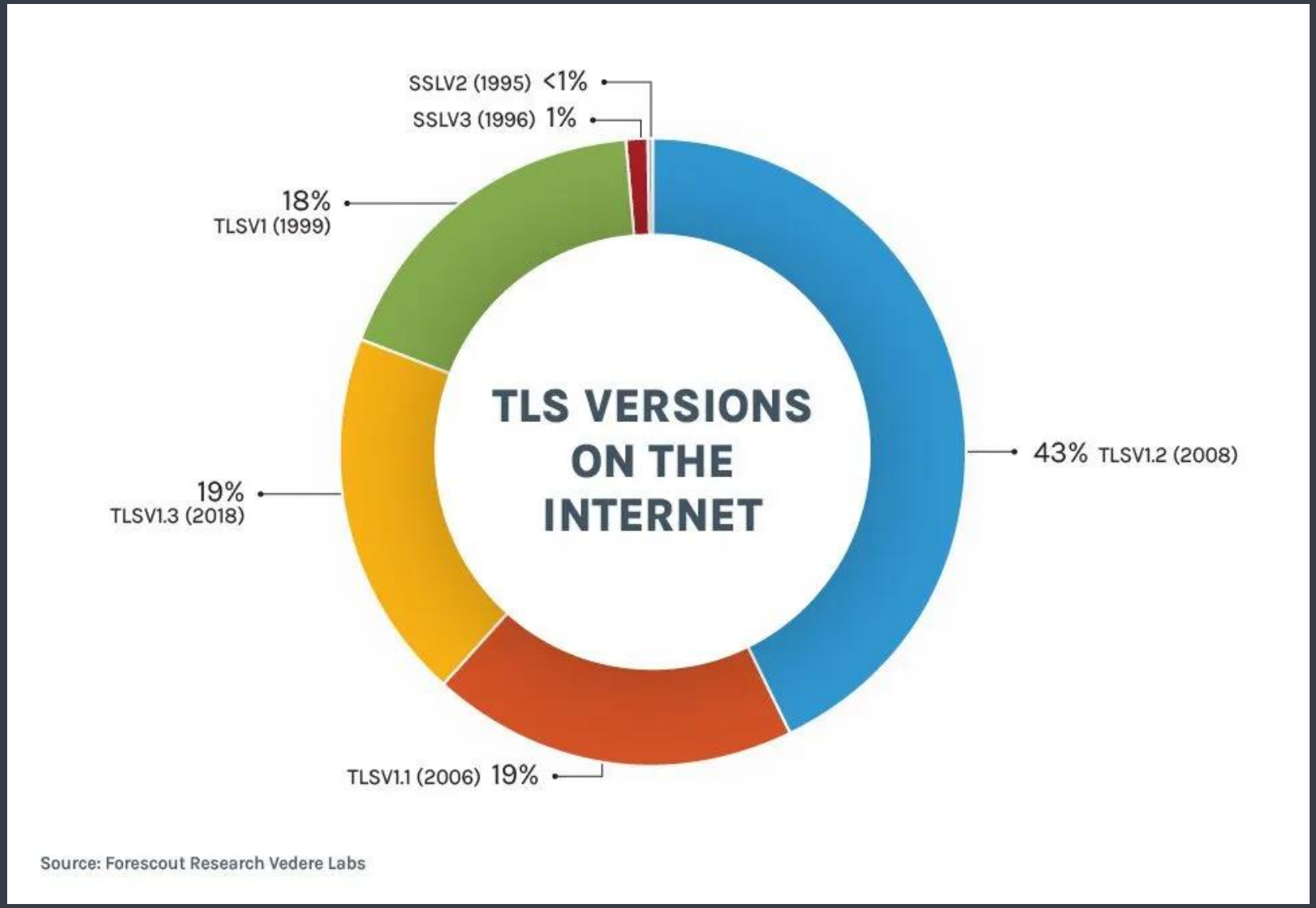
Stateless Hash-Based Digital Signature Standard

(Formerly SPHINCS+) FIPS 205

Next KEM will be HQC. BIKE and Classic McEliece not selected yet. SIKE eliminated. Signatures coming: FALCON and others

protiviti®

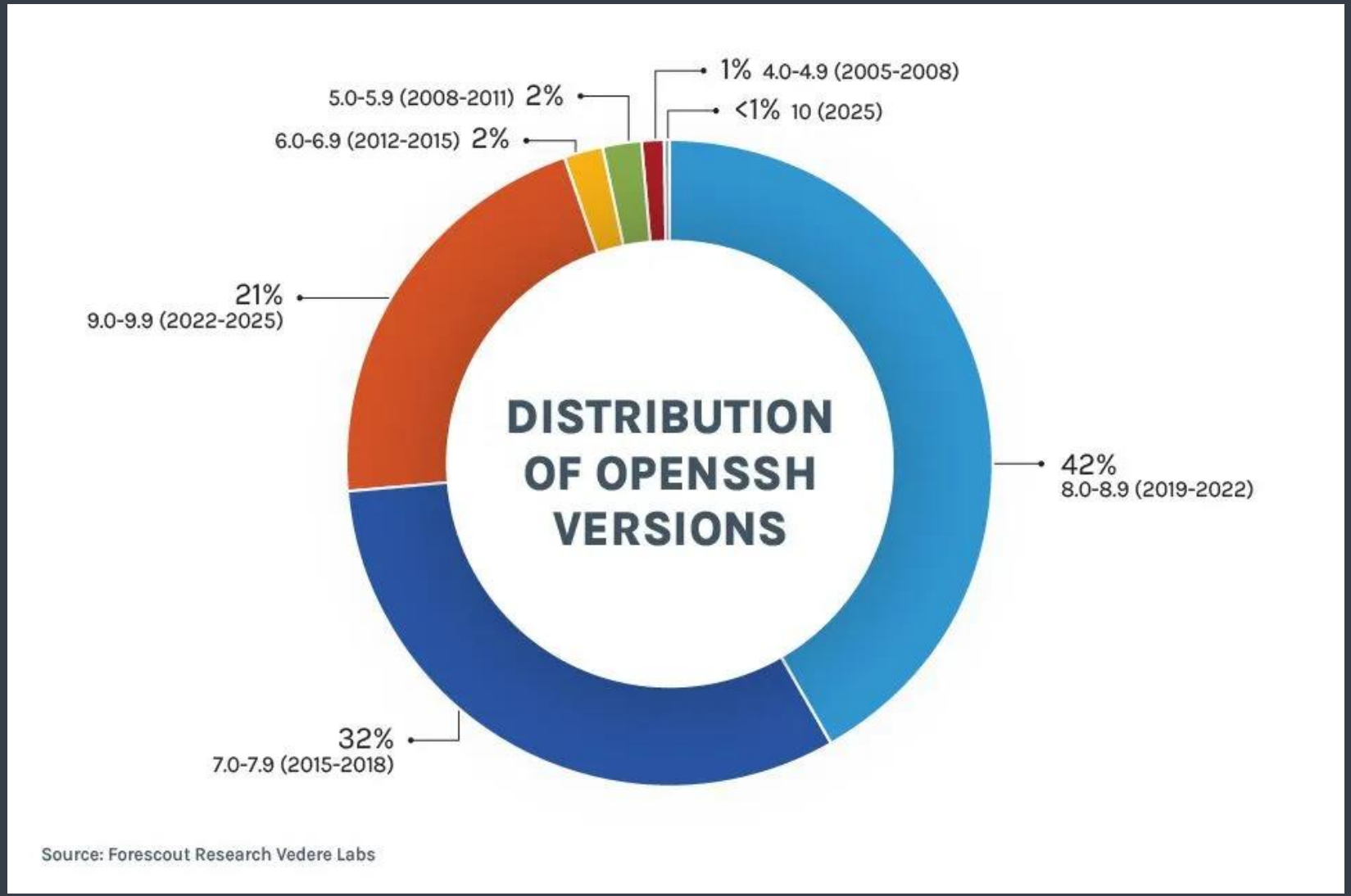
SO HOW ARE WE DOING?



https://www.forescout.com/blog/post-quantum-cryptography-the-real-risks-of-not-adopting-it/

protiviti

SO HOW ARE WE DOING?



protiviti®

DEPRECATION, DISSALLOWED

Family of Algorithms	Parameters	Examples	Transition
Classical Asymmetric Cryptography	112 bits of security strength	RSA (≤2048), ECDH (≤256 bits), ECDSA (≤256 bits)	Deprecated after 2030 Disallowed after 2035
	≥ 128 bits of security strength	RSA (>2048), ECDH (>256 bits), ECDSA (>256 bits)	Disallowed after 2035
Post-Quantum Asymmetric Cryptography	NIST post-quantum security categories 1 to 5	ML-KEM, ML-DSA, SLH-DSA	Allowed
Symmetric Cryptography	112 bits of security strength	SHA-224	Disallowed after 2030
	≥ 128 bits of security strength	SHA-256, AES-128	Allowed

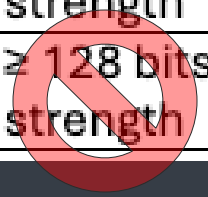
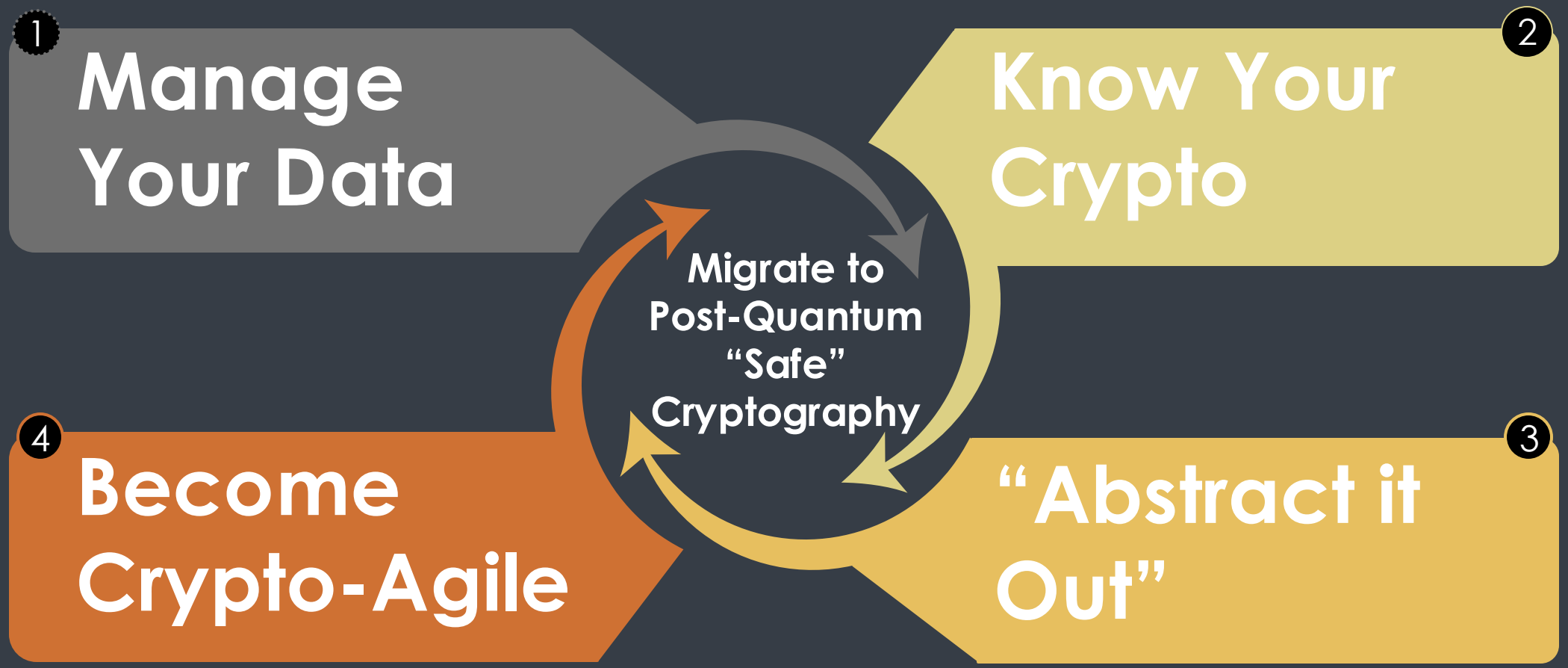


Table based on NIST IR 8547

protiviti

PATH TO CRYPTO AGILITY



protiviti®

QUESTIONS? COME TO QUANTUM VILLAGE @ 5:30



protiviti®