



ISARA

Securing The Future With Quantum-Safe Cryptography

Scott Totzke, CEO & Co-Founder

Alexander Truskovsky, Senior Product Manager

November 16, 2017



Founded in 2015

Headquarters: Waterloo, Ontario, Canada

Full-time employees: 34

- **Decades of commercial experience** in cryptography, security and standards.
- First to market with a **standards-based, commercial quantum safe toolkit**.
- **Mature software development lifecycle** to ensure high-quality, certification ready products for government and financial services.
- **IP Strategy** focused on practical, efficient implementations.
- **Setting the 1st international standards** for quantum safe solutions suitable for large enterprise customers.
- Strong alignment with academic research, the Institute For Quantum computing and the **Quantum Valley Investments ecosystem**.
- Leadership team has **significant business experience and networks** across standards bodies, regulator agencies, government organizations and large enterprises.





PART 1: **UNDERSTANDING THE QUANTUM THREAT**

Scott Totzke, CEO & Co-Founder





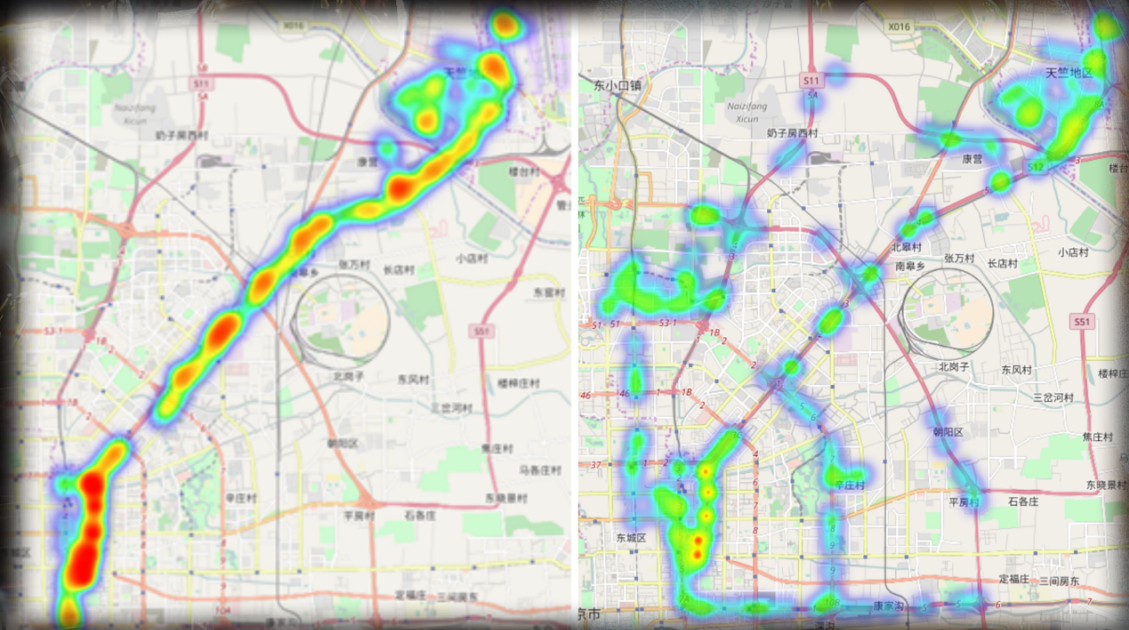
Quantum computing will solve today's
unsolvable problems, opening up

**A NEW REALM OF
POSSIBILITIES.**

CASE STUDY: TRAFFIC FLOW SOLVED

VW IT experts used a D-Wave quantum computer to optimize traffic flow.

10,000 Beijing taxis were intelligently guided to avoid congestion using an algorithm on a quantum computer, significantly reducing their travel time.



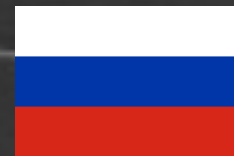
D:WAVE
The Quantum Computing Company™



Source: "Traffic flow optimization using a quantum annealer" <https://arxiv.org/abs/1708.01625>



THE QUANTUM RACE IS ON



Microsoft

Google

rigetti

D-WAVE
The Quantum Computing Company™

IBM



THE CHALLENGE

Quantum computing will break today's
public key encryption standards.

WHAT'S VULNERABLE?

PRODUCTS

VPNs, PKIs, IoT Devices, Vehicles, Apps & CPUs

PROTOCOLS

TLS, IKE, SSH, S/MIME

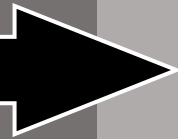
CRYPTOSYSTEMS

RSA, ECC, DH

Confidentiality

Roots of Trust

Identity
Management



A DAY IN LIFE WITHOUT CRYPTOGRAPHY



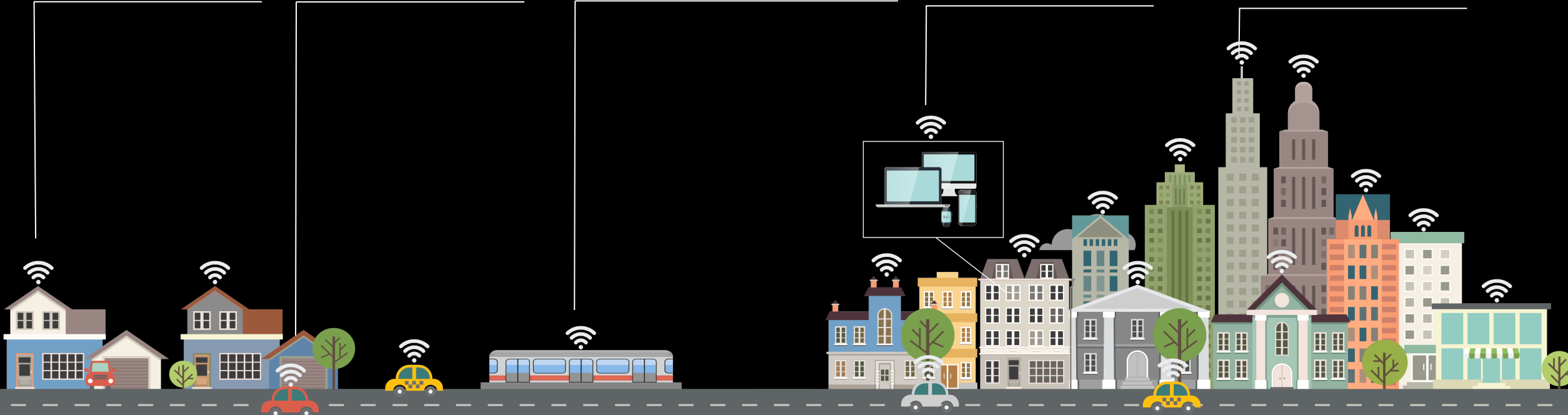
HOME

VEHICLES

TRANSPORTATION

COMPUTING

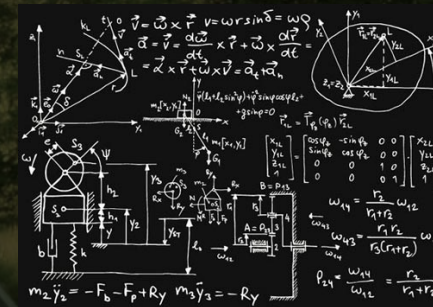
ENTERPRISE



PATHWAYS TO QUANTUM SAFETY



Quantum Key
Distribution



Quantum-Safe
Cryptography

THE “NEW” MATH



Hash-based



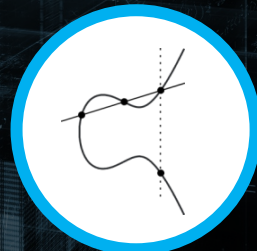
Code-based



Lattice-based



Multivariate-based



Isogeny-based

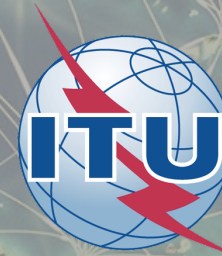


A blurred background image of a large crowd of people walking, likely at a public event or festival, with colorful clothing and motion blur creating a sense of activity and movement.

SUCCESS IS A SEAMLESS (and cost effective) MIGRATION

No Impact to End User Experience

SUCCESS REQUIRES STANDARDS



QUANTUM-SAFE SECURITY IS A STRATEGIC NECESSITY



ISARA's PRODUCTS & SERVICES

RADIATE SECURITY SUITE

Optimized library of quantum-safe algorithms and migration tools.

LICENSING

Custom licensing for OEM's and Security Solutions Developers

PROFESSIONAL SERVICES

Architecture and design
Migration planning
Custom Implementation
Contract Research

TESTING & PILOTING

Full end to end test environment
Pilot set-up and monitoring





PART 2: TECHNICAL DEEP-DIVE

Alexander Truskovsky, Senior Product Manager

WHY CAN'T WE JUST MAKE THE KEY LENGTH LONGER?

| Algorithm | Key Length | Classical Bit Strength | Quantum Bit Strength | Best Quantum Attack |
|-----------|------------|------------------------|----------------------|---------------------|
| RSA 2048 | 2048 bits | 112 bits | 0 bits | Shor's |
| RSA 3072 | 3072 bits | 128 bits | 0 bits | Shor's |
| ECC 256 | 256 bits | 128 bits | 0 bits | Shor's |
| ECC 521 | 521 bits | 256 bits | 0 bits | Shor's |
| AES 128 | 128 bits | 128 bits | 64 bits | Grover's |
| AES 256 | 256 bits | 256 bits | 128 bits | Grover's |
| SHA 256 | 256 bits | 256 bits | 128 bits | Grover's |

HOW ARE SECURE COMMUNICATIONS VULNERABLE?



Secure Communication Protocol



Handshake

Data Exchange



Shor's algorithm **breaks**
current public-key algorithms

Authentication
Key Establishment

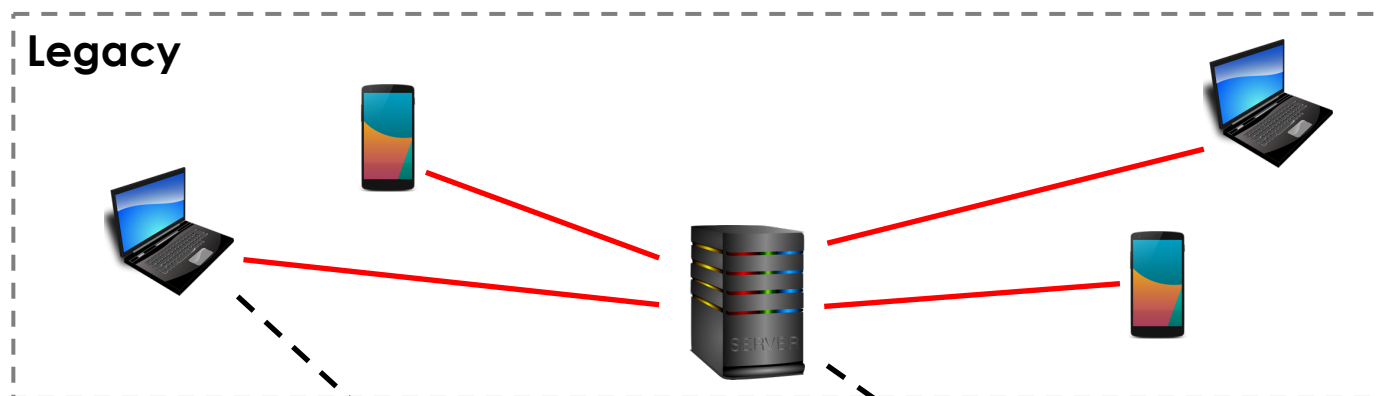


Symmetric Encryption
AES 256 → AES 128

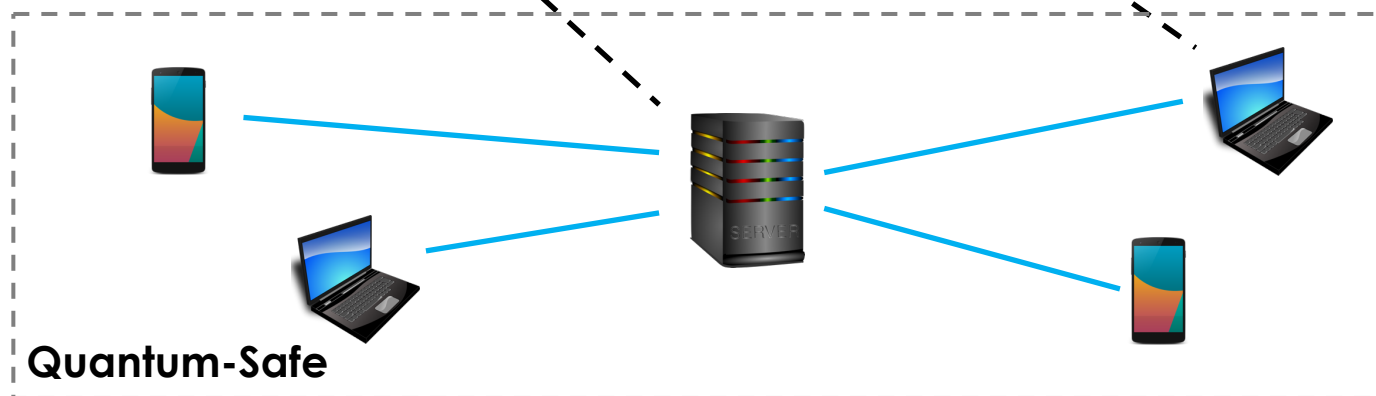
Grover's algorithm **reduces** the
effective symmetric key size to half

MIGRATION WILL TAKE YEARS

Classic
Connection



Quantum-Safe
Connection



QUANTUM-SAFE OPTIONS

| Approach | Quantum-Safe Option | Digital Signature | Public-Key Encryption | Key Agreement |
|-------------|--------------------------------|-------------------|-----------------------|---------------|
| Mathematics | Hashes | ✓ | | |
| | Lattices | ✓ | ✓ | ✓ |
| | Error Correcting Codes | ✓ | ✓ | |
| | Isogeny | ✓ | ✓ | ✓ |
| | Multivariate | ✓ | ✓ | |
| Physics | Quantum Key Distribution (QKD) | | | ✓ |

QUANTUM KEY DISTRIBUTION (QKD)

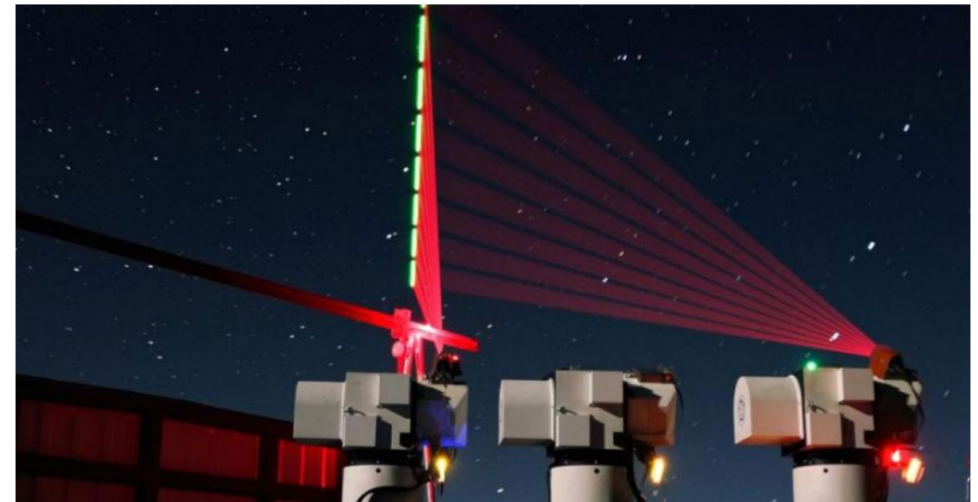
- Utilize physics for key distribution
- Requires a fibre optic connection or line of sight
- Serious distance restrictions
- Side channel risks
- Still requires an authentic channel protected by quantum-resistant cryptography

finance.yahoo.com

China uses a quantum satellite to transmit potentially unhackable info for the first time ever

Arjun Kharpal

4-5 minutes



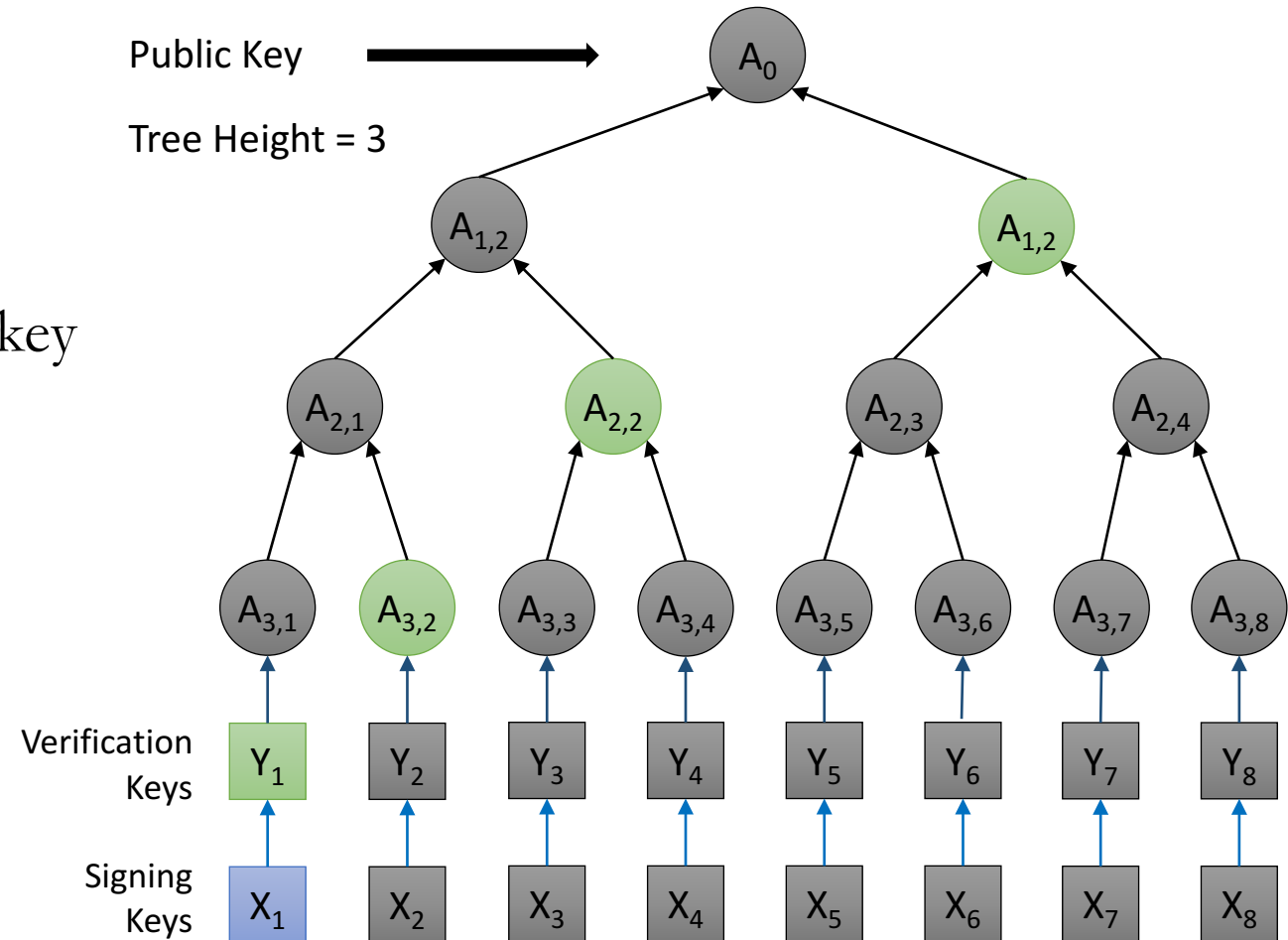
“There is an emerging consensus that the best practical approach to quantum security is to evolve current security applications and packet-based communication protocols towards adopting post-quantum public key cryptography. Software or firmware implementations of post-quantum cryptography should be easier to develop, deploy and maintain, have lower lifecycle support costs, and have better understood security threats than QKD-based solutions.”

From Quantum Key Distribution – A CESG Whitepaper
Published: February 2016



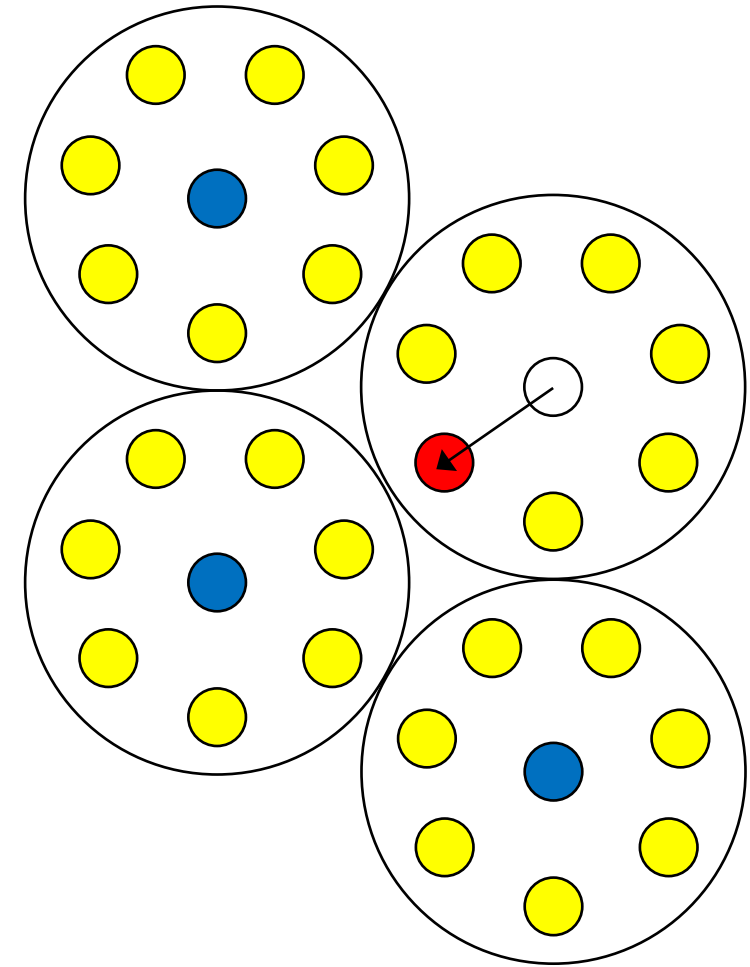
HASH-BASED CRYPTOGRAPHY

- Introduced by Merkle in 1979
- “One-Time Signatures”
- Small public key but very large private key
- Fast signing & verifying
- Stateful
- Candidates:
 - Leighton-Micali Signatures (LMS)
 - eXtended Merkle Signature Scheme (XMSS)
 - SPHINCS



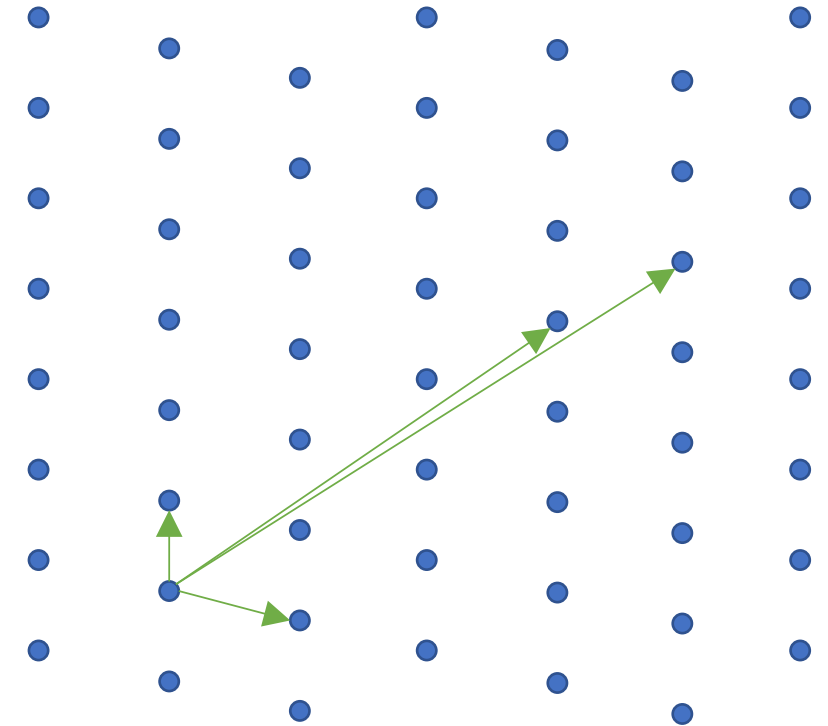
CODE-BASED CRYPTOGRAPHY

- Introduced by McEliece in 1978
- Relies on hardness of decoding unknown codes
- Very large public keys
- Fast encryption and decryption
- Smaller variants – QC-MDPC, McBits, others
- Recent attacks mitigated through ephemeral use



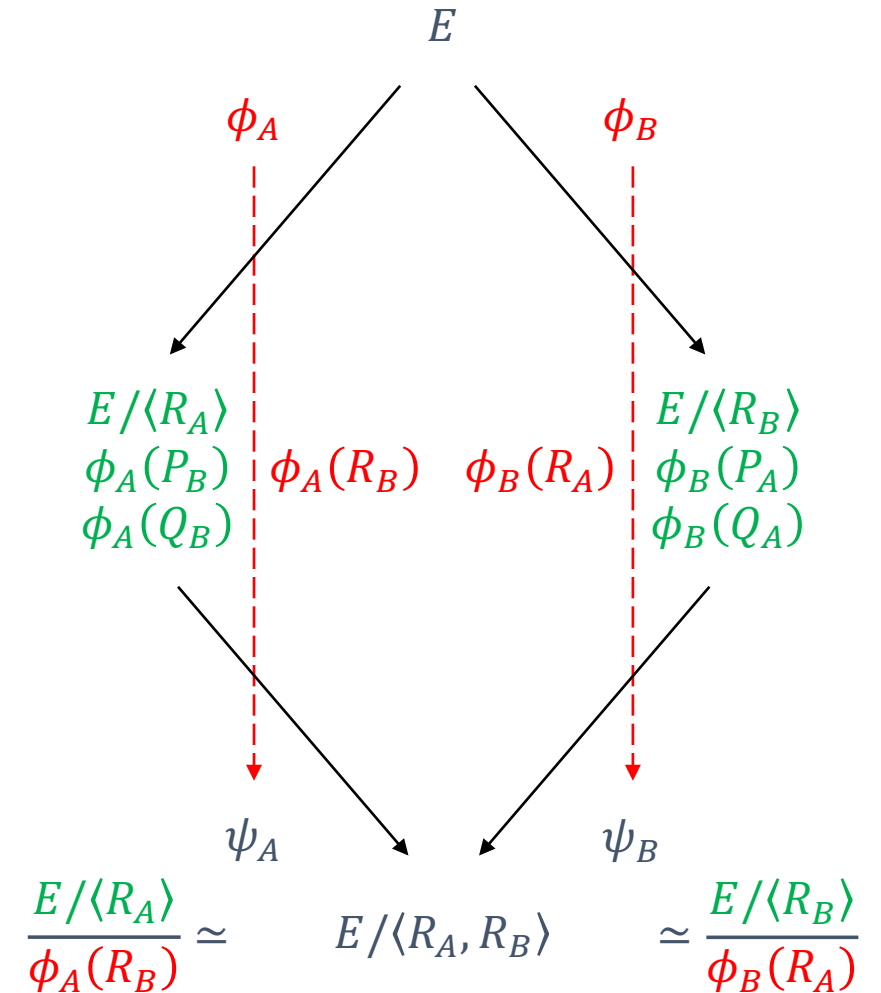
LATTICE-BASED CRYPTOGRAPHY

- First commercial version was NTRU (1996)
- Two most important hard problems:
 - Shortest Integer Solution (SIS)
 - Learning With Errors (LWE)
- Competitive key sizes and fast operations
- Open questions around tightness of reductions
- Risks when used in a static or static/ephemeral environment
- Google public experiments with NewHope in Chrome Canary



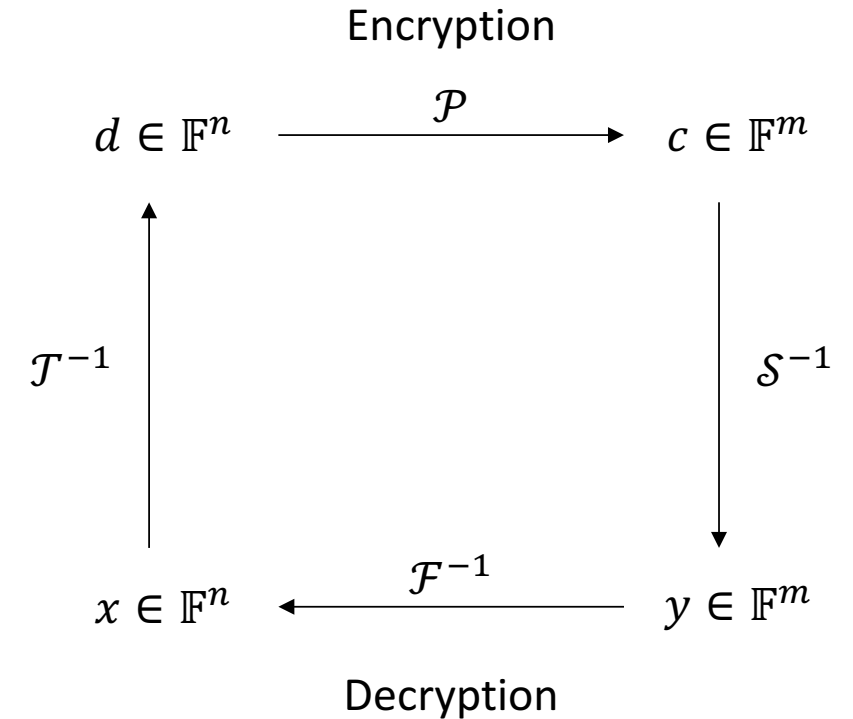
ISOGENY-BASED CRYPTOGRAPHY

- Introduced by Jao in 2009
- Relies on difficulty of finding isogenies (mappings) between Elliptic Curves
- Competitive key sizes
- Slower operations
- Risks when used in a static or static/ephemeral way



MULTIVARIATE-BASED CRYPTOGRAPHY

- Introduced by Matsumoto and Imai in 1988
- Based on the fact that solving n randomly chosen (non-linear) equations in n variables is NP-complete
- Can be formulated into signatures, key exchange and key transport
- Often trade offs between key size and public/private key operation speeds



CHALLENGES TO QUANTUM-SAFE SECURITY

- It takes **several years of cryptanalysis** for cryptographers to gain confidence in the security of new algorithms
- Some network security protocols **may be too rigid** to accommodate the increased key lengths or changes in ciphers required to make them quantum-safe
- **New standards** for protocols are needed
- Many people perceive quantum-safe cryptography as “not urgent,” despite the **lead times required** to analyze new cryptosystems and implement them

STANDARDS: NIST

Fall 2016: Formal call for quantum-resistant public key crypto standards

November 2017: Deadline for submissions

3-5 years later: Analysis phase

2 years later: Draft standards ready



STANDARDS: ETSI

Industry Specifications Groups

- Quantum Safe Cryptography (QSC)
- Quantum Key Distribution (QKD)

Focus on practical implementation of quantum safe primitives

- Performance considerations
- Implementation capabilities
- Benchmarking
- Practical architectural considerations



STANDARDS: ISO SC27

- Interest focused within SC27 group
- Call for contributions out being lead by Lily Chen
- Liaisons with groups such as ETSI Quantum Safe Working Group
- Mostly at a study group phase



STANDARDS: ITU

- A contribution submitted by Canada was **approved** that proposes the inclusion of optional support for multiple public-key algorithms in Recommendation ITU-T X509 | ISO/IEC 9594-8.



STANDARDS: IETF

- Post-quantum Preshared Keys for IKEv2
- Quantum-Safe Hybrid (QSH) Ciphersuite for Transport Layer Security (TLS) version 1.3
- Use of the Hash-based Merkle Tree Signature (MTS) Algorithm in the Cryptographic Message Syntax (CMS)
- Hybrid Quantum-Safe Key Exchange for Internet Key Exchange Protocol Version 2 (IKEv2)



STANDARDS: X9

- TR-50 Quantum Techniques in Cryptographic Messaging Syntax (CMS)
- TR-50 will define ASN.1 schema and associated processing procedures for using 'quantum-safe' cryptographic algorithms, mechanisms, and techniques in the cryptographic message syntax (CMS) defined in X9.73. The resulting TR will enable financial services institutions to begin preparing for migrations to quantum-safe control solutions that rely on CMS and enable the industry to pursue proof-of-concept and testing activities.



CLEARING THE PATH TO QUANTUM-SAFE SECURITY

www.isara.com
quantumsafe@isara.com



Scott Totzke
CEO & Co-Founder
scott@isara.com



Alexander Truskovsky
Senior Product Manager
alex@isara.com

Join us on social



@ISARACorp



@ISARACorp



@ISARA Corporation





ISARA