

Emerging Topics in Network Security: Post-Quantum Security

Outline

- **The Quantum Threat to Cryptography**
- **Post-Quantum Cryptography**
- **PQC Standardization and Migration**
- **Big Questions**

Basic Cryptographic Primitives

- **Integrity:** hash functions
 - ~~SHA-1~~, ~~MD5~~, SHA-2, SHA-3
- **Authenticity:** MACs and digital signatures
 - HMAC, RSA, DSA, ECDSA
- **Confidentiality:** SKE and PKE/KEX/KEM
 - ~~DES~~, AES, DH, ECDH, ECIES, ElGamal, RSA, etc.

Public-Key Cryptography

- Two mathematically related keys: pk, sk
 - $c = ENC(pk, m) \rightarrow m = DEC(sk, c)$
 - $s = SIG(sk, m) \rightarrow VER(pk, s, m) = 1$
- Computational assumptions
 - Necessary: Given pk , it is infeasible to compute sk .
 - Widely used assumptions:
 - Factoring integers is hard
 - Computing discrete logarithms in some group is hard
- What does “hard” mean?
 - $Factoring \notin P, DiscreteLog \notin P, EC DL \notin P$

Quantum Algorithms

- **Shor's algorithm (1994)**

- Factors an integer **N** in time $\tilde{O}(\log^3 N)$
- Computes discrete log in a group of size **N** in time $\tilde{O}(\log^3 N)$



Image source:
Wikipedia

Algorithms for Quantum Computation: Discrete Logarithms and Factoring

Peter W. Shor
AT&T Bell Labs
Room 2D-149
600 Mountain Ave.
Murray Hill, NJ 07974, USA

Abstract

A computer is generally considered to be a universal computational device; i.e., it is believed able to simulate any physical computational device with a cost in computation time of at most a polynomial factor. It is not clear whether this is still true when quantum mechanics is taken into consideration. Several researchers, starting with David Deutsch, have developed models for quantum mechanical computers and have investigated their computational properties. This paper gives Las Vegas algorithms for finding discrete logarithms and factoring integers on a quantum computer that take a number of steps which is polynomial in the input size, e.g., the number of digits of the integer to be factored. These two problems are generally considered hard on a classical computer and have been used as the basis of several proposed cryptosystems. (We thus give the first examples of quantum cryptanalysis.)

[1, 2]. Although he did not ask whether quantum mechanics conferred extra power to computation, he did show that a Turing machine could be simulated by the reversible unitary evolution of a quantum process, which is a necessary prerequisite for quantum computation. Deutsch [9, 10] was the first to give an explicit model of quantum computation. He defined both quantum Turing machines and quantum circuits and investigated some of their properties.

The next part of this paper discusses how quantum computation relates to classical complexity classes. We will thus first give a brief intuitive discussion of complexity classes for those readers who do not have this background. There are generally two resources which limit the ability of computers to solve large problems: time and space (i.e., memory). The field of analysis of algorithms considers the asymptotic demands that algorithms make for these resources as a function of the problem size. Theoretical computer scientists generally classify algorithms as eff-

Quantum Algorithms

- **Grover's algorithm (1996)**
 - Searches an unsorted database of size N in time $O(\sqrt{N})$
 - “Optimal”: lower bound $\Omega(\sqrt{N})$ [BBBV-1994]



A fast quantum mechanical algorithm for database search

Lov K. Grover
3C-404A, AT&T Bell Labs
600 Mountain Avenue
Murray Hill NJ 07974
lkg@mhcnet.att.com

Summary

An unsorted database contains N records, of which just one satisfies a particular property. The problem is to identify that one record. Any classical algorithm, deterministic or probabilistic, will clearly take $O(N)$ steps since on the average it will have to examine a large fraction of the N records. Quantum mechanical systems can do several operations simultaneously due to their wave like properties. This paper gives an $O(\sqrt{N})$ step quantum mechanical algorithm for identifying that record. It is within a constant factor of the fastest possible quantum mechanical algorithm.

This paper applies quantum computing to a mundane problem in information processing and presents an algorithm that is significantly faster than any classical algorithm can be. The problem is this: there is an unsorted database containing N items out of which just one item satisfies a given condition - that one item has to be retrieved. Once an item is examined, it is possible to tell whether or not it satisfies the condition in one step. However, there does not exist any sorting on the database that would aid its selection. The most efficient classical algorithm for this is to examine the items in the database one by one. If an item satisfies the required condition stop; if it does not, keep track of this item so that it is not examined again. To be certain you

Cryptosystem	Category	Key Size	Security Parameter	Quantum Algorithm Expected to Defeat Cryptosystem	# Logical Qubits Required	# Physical Qubits Required ^a	Time Required to Break System ^b
AES-GCM ^c	Symmetric encryption	128 192 256	128 192 256	Grover's algorithm	2,953 4,449 6,681	4.61×10^6 1.68×10^7 3.36×10^7	2.61×10^{12} years 1.97×10^{22} years 2.29×10^{32} years
RSA ^d	Asymmetric encryption	1024 2048 4096	80 112 128	Shor's algorithm	2,050 4,098 8,194	8.05×10^6 8.56×10^6 1.12×10^7	3.58 hours 28.63 hours 229 hours
ECC Discrete-log problem ^{e-g}	Asymmetric encryption	256 384 521	128 192 256	Shor's algorithm	2,330 3,484 4,719	8.56×10^6 9.05×10^6 1.13×10^6	10.5 hours 37.67 hours 55 hours
SHA256 ^h	Bitcoin mining	N/A	72	Grover's Algorithm	2,403	2.23×10^6	1.8×10^4 years

Source: National Academies of Sciences, Engineering, and Medicine 2019. Quantum Computing: Progress and Prospects. Washington, DC: The National Academies Press.

Google demonstrates vital step towards large-scale quantum computers



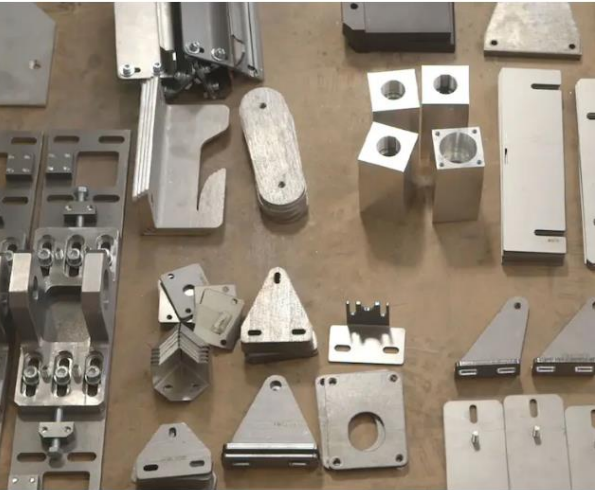
TECHNOLOGY 14 July 2021
By Matthew Sparkes



Google's Sycamore quantum computer
RETURN CAGLIARI/CONTRASTO

IBM's roadmap for scaling quantum technology

Our quantum roadmap is leading to increasingly larger and better chips, with a 1,000-qubit chip, IBM Quantum Condor, targeted for the end of 2023.

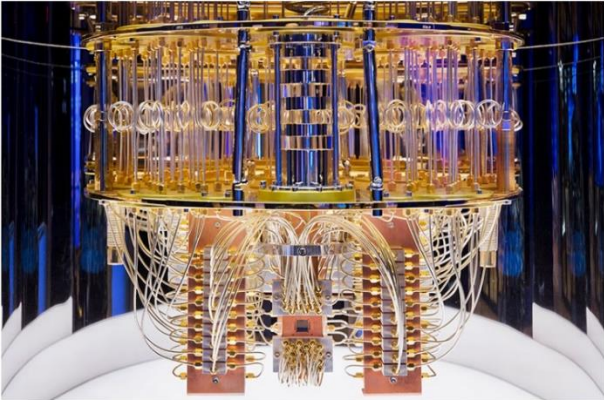


NEWS | 19 November 2021

First quantum computer to pack 100 qubits enters crowded race

But IBM's latest quantum chip and its competitors face a long path towards making the machines useful.

Philip Ball



The innards of an IBM quantum computer show the tangle of cables used to control and read out its

Quantum computers may be able to break Bitcoin sooner than you think

By Joel Khalili published February 05, 2022

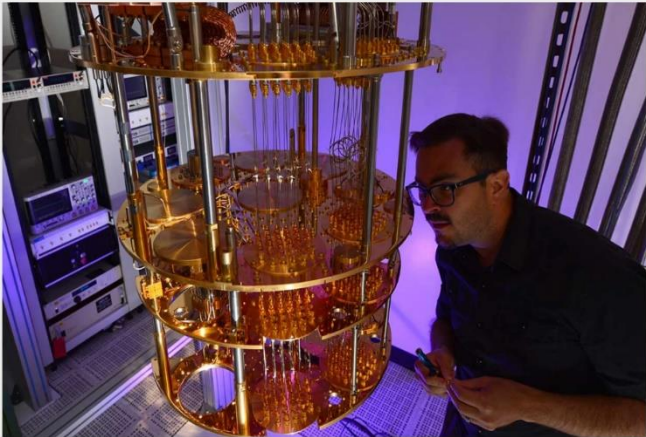
New research suggests quantum machines with 13 million qubits could crack Bitcoin encryption



(Image credit: Shutterstock / REDPIXEL.PL)

What Intel Is Planning for The Future of Quantum Computing: Hot Qubits, Cold Control Chips, and Rapid Testing > Director of quantum hardware, Jim Clarke explains the company's path toward "quantum practicality"

BY SAMUEL K. MOORE | 24 AUG 2020 | 10 MIN READ |



Intel quantum-computing researcher David Michalak inspects part of a quantum computing system at the company's Hillsboro, Ore., campus. PHOTO: WALDEN KIROCH/INTEL CORP.

Two of World's Biggest Quantum Computers Made in China > Quantum computers Zuchongzi and Jiuzhang 2.0 may both display "quantum primacy" over classical computers

BY CHARLES Q. CHOI | 06 NOV 2021 | 2 MIN READ |

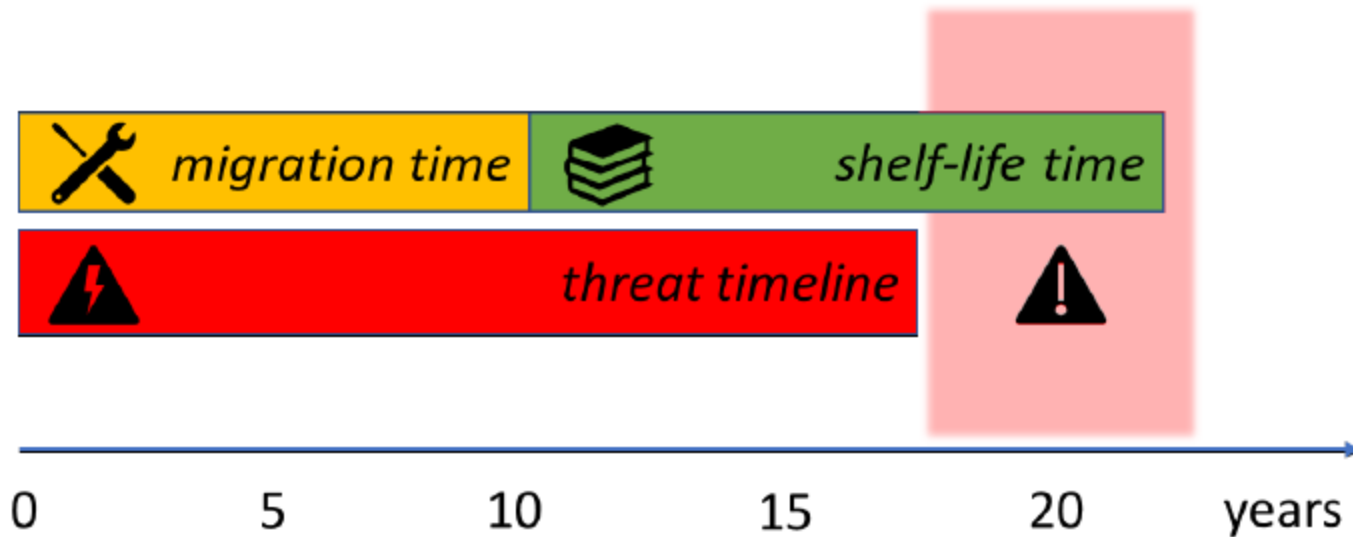


Chinese optical quantum computer Jiuzhang 2.0 can solve a problem 10^24 faster than a classical computer. CHAO-YANG LIU/UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA

How Quantum Computers May Affect Network Security Protocols?

- Diffie-Hellman key exchange?
- RSA encryption/signature?
- Kerberos?
- IPSec?
- TLS?
- SSH?
- PGP, S/MIME?

Quantum Threats to Cryptography



Source: Mosca and Piani, 2021 Quantum Threat Timeline Report, Global Risk Institute

Example: migration = 10 y, shelf-life = 20 y, threat = 28 y
→ 2 “insecure” years

Experts: It is likely that within 25-30 years, quantum computers can break RSA-2048 in 24h [2021 Quantum Threat Timeline Report, GRI]

Quantum Threats to Cryptography

- Grover's algorithm: Weakens symmetric-key cryptography
 - **Double the key sizes of AES, SHA**
- Shor's algorithm: Breaks current public-key cryptography
 - Increase key sizes: “post-quantum RSA” [BHLV-2017], key size 1TB
- **Post-quantum cryptography**
 - Believed to be **secure against both classical and quantum computers**
 - Can be efficiently implemented on classical computers
 - Based on alternative foundations

Post-Quantum Cryptography

- Lattices
- Codes
- Multivariates
- Isogenies
- Hashes, block ciphers
- Etc.

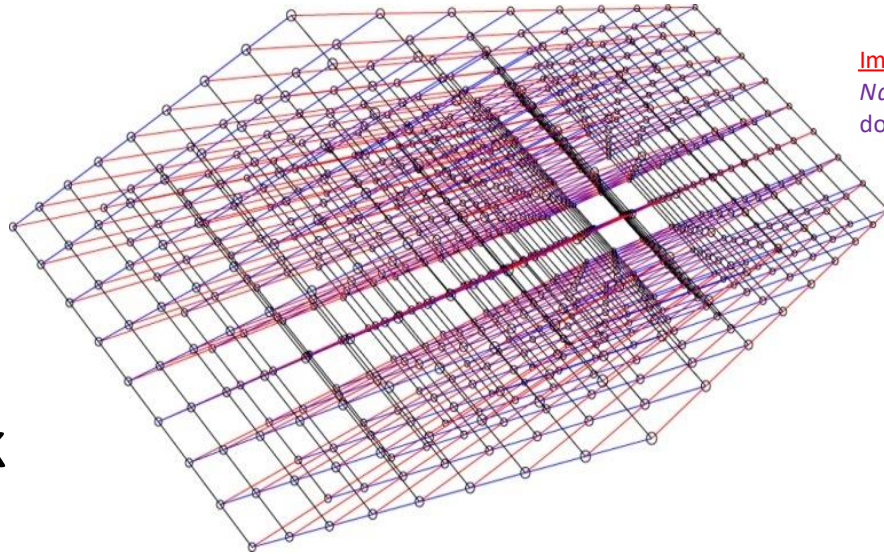


Image source: Bernstein-Lange,
Nature **549**, 188–194 (2017)
doi:10.1038/nature23461

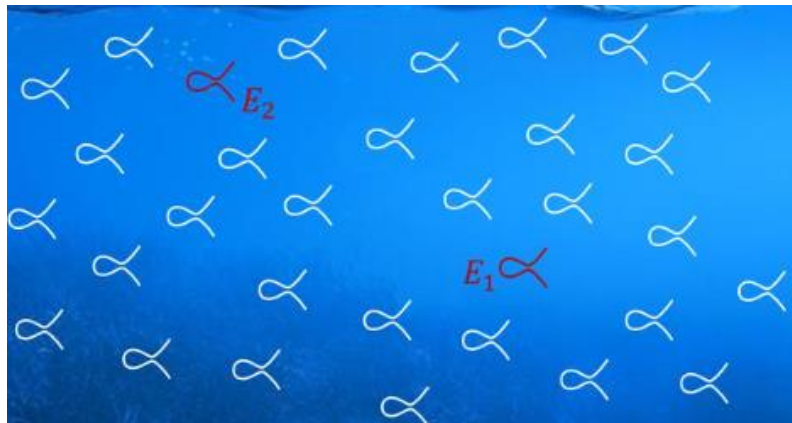


Image source: Castryck, 2018

“Noisy Problems”

The diagram illustrates the noisy problem equation: $\mathbf{b} = \mathbf{A}^T \mathbf{s} + \mathbf{e} \pmod{q}$. Matrix \mathbf{A} is a pink rectangle with dimensions n (height) and m (width). Vector \mathbf{b} is a blue vertical bar. Matrix \mathbf{A}^T is a pink rectangle. Vector \mathbf{s} is a green vertical bar. Vector \mathbf{e} is an orange vertical bar. The error vector \mathbf{e} is bounded by $\|\mathbf{e}\|_\infty \leq \beta$.

- **Lattices:** Learning with Errors (LWE) [Regev, 2005]
- **Codes:** Decoding linear codes [McEliece, Berlekamp et al., 1978]
- Variants to improve efficiency

PQC Standardizations

- **IEEE P1363.1**: lattice-based PKE (2008)
- **IETF**: stateful hash-based signatures
- **ANSI**: recommendations on lattice-based algorithms (2010)
- **ETSI, ISO/IEC JTC 1/SC 27**: reports/documents on PQC
- **EU expert groups PQCRYPTO, SAFEcrypto**: reports on PQC
- **Some countries**: USA, China
- **NIST's Standardization Process**

NIST's PQC Project

- **Targets:** A set of recommended post-quantum basic algorithms (signatures, PKE/KEMs) for the long-term future
- **Timeline:**
 - Feb 2016: Announcement
 - Nov 2017: 1st round (82 submissions, 69 eligible, 25 broken)
 - Jan 2019: 26 proposals invited to 2nd round (8 broken)
 - Jul 2020: Round 3 announcement
 - **7 finalists:** most promising algorithms (1 partially broken)
 - **8 alternates:** candidates for potential standardization
 - July 2022: **Winners announced**
 - August 2024: **PQC Standards released**

NIST's PQC Project: Round 3 Finalists

Type	PKE/KEM	Signature
Lattice ^[a]	<ul style="list-style-type: none">• CRYSTALS-Kyber• NTRU• SABER	<ul style="list-style-type: none">• CRYSTALS-Dilithium• FALCON
Code-based	<ul style="list-style-type: none">• Classic McEliece	
Multivariate		<ul style="list-style-type: none">• Rainbow

Table source:
Wikipedia

- **Kyber, NTRU, SABER**: good performance (efficiency, key/ciphertext sizes)
→ 1 will likely be selected as KEM standard
- **Classic McEliece**: large public keys
- **Rainbow** (large public keys) has recently been attacked [Beullens, 2022]
- One of **Dilithium** and **FALCON** will likely be selected

NIST's PQC Project: Round 3 Alternates

Type	PKE/KEM	Signature
Lattice	<ul style="list-style-type: none">• FrodoKEM• NTRU Prime	
Code-based	<ul style="list-style-type: none">• BIKE• HQC	
Hash-based		<ul style="list-style-type: none">• SPHINCS+
Multivariate		<ul style="list-style-type: none">• GeMSS
Supersingular elliptic curve isogeny	<ul style="list-style-type: none">• SIKE	
Zero-knowledge proofs		<ul style="list-style-type: none">• Picnic

Table source:
Wikipedia

- **SPHINCS+, Picnic**: high confidence in (post-quantum) security
→ **SPHINCS+** will likely be standardized separately.
- NIST will additionally call for (non-lattice-based) signatures

NIST's PQC Project: Round-3 Winners

On July 5, 2022, NIST announced the first group of winners from its six-year competition.

Type	PKE/KEM	Signature
Lattice	<ul style="list-style-type: none">CRYSTALS-Kyber	<ul style="list-style-type: none">CRYSTALS-Dilithium ↗FALCON ↗
Hash-based		<ul style="list-style-type: none">SPHINCS+ ↗

NIST's PQC Project: Round 4

On July 5, 2022, NIST announced four candidates for PQC Standardization Round 4

Type	PKE/KEM
Code-based	<ul style="list-style-type: none">• BIKE• Classic <u>McEliece</u>• HQC
<u>Supersingular elliptic curve isogeny</u>	<ul style="list-style-type: none">• SIKE (Broken August 5, 2022)

On March 11, 2025, NIST announced the selection of a backup algorithm for KEM.

Type	PKE/KEM
Code-based	HQC

NIST's PQC Project: Standards

- FIPS 203: standard for general encryption. Based on CRYSTALS-Kyber, renamed as ML-KEM.
- FIPS 204: standard for digital signatures. Based on CRYSTALS-Dilithium, renamed as ML-DSA.
- FIPS 205: standard for digital signatures. Based on SPHINCS+, renamed as SLH-DSA.
- FIPS 206: standard for digital signatures. Based on FALCON, renamed as FN-DSA

Migration to Post-Quantum Cryptography

The advent of quantum computing technology will compromise many of the current cryptographic algorithms, especially public-key cryptography, which is widely used to protect digital information. Most algorithms on which we depend are used worldwide in components of many different communications, processing, and storage systems. Once access to practical quantum computers becomes available, all public-key algorithms and associated protocols will be vulnerable to criminals, competitors, and other adversaries. It is critical to begin planning for the replacement of hardware, software, and services that use public-key algorithms now so that information is protected from future attacks.

[READ OUR PROJECT FAQ](#)

Initiating the development of practices to ease migration from the current set of public-key cryptographic algorithms to replacement algorithms that are resistant to quantum computer-based attacks

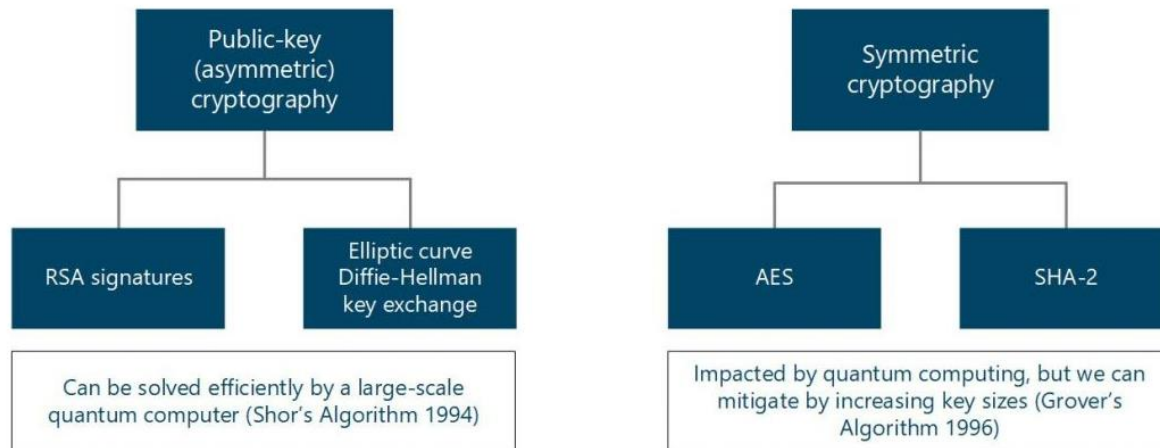
The project has two workstreams. The Cryptographic Discovery workstream is focused on the use of cryptographic inventory tools to allow an organization to learn where and how cryptography is being used to protect the confidentiality and integrity of your organization's important data and digital systems. The discovery workstream is also looking at how cryptographic inventories can support risk management and prioritization decisions about where to implement the technologies that leverage the NIST standardized post-quantum cryptographic algorithms. The Interoperability and Performance workstream explores how the NIST PQC algorithms for key establishment and digital signature schemes will operate in communication protocols such as the Transport Layer Security (TLS) protocol, the Secure Shell (SSH) protocol and with hardware security modules (HSMs). The Interoperability and Performance workstream answers questions about how the soon-to-be standardized PQC algorithms will operate in communication protocols such as the Transport Layer Security (TLS) protocol and the Secure Shell (SSH) protocol and in hardware security modules (HSMs).

Post-Quantum TLS

People

The Transport Layer Security (TLS) protocol

The Transport Layer Security (TLS) protocol is one of the most widely-used security protocols in use today, protecting the information exchanged between web clients and servers all around the world. While TLS is secure against today's classical computers, the asymmetric cryptography in TLS is unfortunately vulnerable to future attacks from quantum computers.





Quantum-safe cryptography in TLS

Last updated 2024-09-18

You can use a quantum safe enabled TLS connection to send requests to a IBM® Key Protect for IBM Cloud® service endpoint.

What is Quantum Safe Cryptography?

Quantum safe cryptography, also known as post quantum cryptography, is a new generation of the public-key cryptographic system that is undergoing NIST evaluation. These new quantum cryptographic algorithms are based on hard mathematical problems that based on current research, even large quantum computers cannot break.

When these quantum cryptographic algorithms are used for TLS communication, the security of the public key exchange between the client and server are expected to have higher security levels than the current RSA and ECC algorithms. However, NIST has not standardized the algorithms and until then, Key Protect has adopted a hybrid method that combines both Quantum Safe and current ECC algorithms to protect in-transit data.

Why is Quantum Safe TLS important?

As quantum computing continues to evolve and advance, a large quantum computer will be able to run a ["SHOR" algorithm](#) that can break the current TLS communication algorithms (RSA/ECC) in a matter of minutes. While large quantum computers are not available today, any TLS data-in-transit that has been snooped and stored can be breached when these large quantum computers are made available. Data has a long shelf life so it is critical that Key Protect supports quantum safe cryptographic algorithms to secure TLS communications.

To keep your in-transit data resilient, Key Protect has introduced the ability to use a quantum safe enabled TLS connection to ensure that your data is secure during the key exchange process.

What are the considerations of Quantum Safe Cryptography?

Before configuring your service to send requests to Key Protect through a quantum safe enabled Key Protect service endpoint, please keep in mind the following considerations:

- The National Institute for Standards and Technology (NIST) is in the process of [standardizing quantum safe algorithms](#). NIST is currently evaluating candidate approaches to quantum safe cryptography and isn't expected to complete the standardization process until after 2023. Key Protect uses the [Kyber algorithm](#), which is one of the third round candidates under evaluation. If NIST's research reveals that the Kyber algorithm



What is Quantum Safe Cryptography?

Why is Quantum Safe TLS important?

What are the considerations of Quantum Safe Cryptography?

Using Quantum Safe TLS with Key Protect

Configure Quantum Safe TLS with Key Protect via the SDK

Using Quantum Safe Key Protect endpoints via CURL

POSTED ON MAY 22, 2024 TO [SECURITY](#)

Post-quantum readiness for TLS at Meta



Using hybrid post-quantum TLS with AWS KMS

[PDF](#) | [RSS](#)

AWS Key Management Service (AWS KMS) supports a hybrid post-quantum key exchange option for the Transport Layer Security (TLS) network encryption protocol. You can use this TLS option when you connect to AWS KMS API endpoints. We're offering this feature before post-quantum algorithms are standardized so you can begin testing the effect of these key exchange protocols on AWS KMS calls. These optional hybrid post-quantum key exchange features are at least as secure as the TLS encryption we use today and are likely to provide additional long-term security benefits. However, they affect latency and throughput compared to the classic key exchange protocols in use today.

The data that you send to AWS Key Management Service (AWS KMS) is protected in transit by the encryption provided by a Transport Layer Security (TLS) connection. The classic cipher suites that AWS KMS supports for TLS sessions make brute force attacks on the key exchange mechanisms infeasible with current technology. However, if large-scale quantum computing becomes practical in the future, the classic cipher suites used in TLS key exchange mechanisms will be susceptible to these attacks. If you're developing applications that rely on the long-term confidentiality of data passed over a TLS connection, you should consider a plan to migrate to post-quantum cryptography before large-scale quantum computers become available for use. AWS is working to prepare for this future, and we want you to be well-prepared, too.

To protect data encrypted today against potential future attacks, AWS is participating with the cryptographic community in the development of quantum-resistant or *post-quantum* algorithms. We've implemented *hybrid* post-quantum key exchange cipher suites in AWS KMS that combine classic and post-quantum elements to ensure that your TLS connection is at least as strong as it would be with classic cipher suites.

These hybrid cipher suites are available for use on your production workloads in [most AWS Regions](#). However, because the performance characteristics and bandwidth requirements of hybrid cipher suites are different from those of classic key exchange mechanisms, we recommend that you [test them on your AWS KMS API calls](#) under different conditions.

Feedback

As always, we welcome your feedback and participation in our open-source repositories. We'd especially like to hear how your infrastructure interacts with this new variant of TLS traffic.

- To provide feedback on this topic, use the **Feedback** link in the upper right corner of this page.
- We're developing these hybrid cipher suites in open source in the [s2n-tls](#) repository on GitHub. To provide feedback on the usability of the cipher suites, or share novel test conditions or results, [create an issue](#) in the s2n-tls repository.
- We're writing code samples for using hybrid post-quantum TLS with AWS KMS in the [aws-kms-pq-tls-example](#) GitHub repository. To ask questions or share ideas about configuring your HTTP client or AWS KMS client to use the hybrid cipher suites, [create an issue](#) in the aws-kms-pq-tls-example repository.

Supported AWS Regions



Big Theoretical Questions

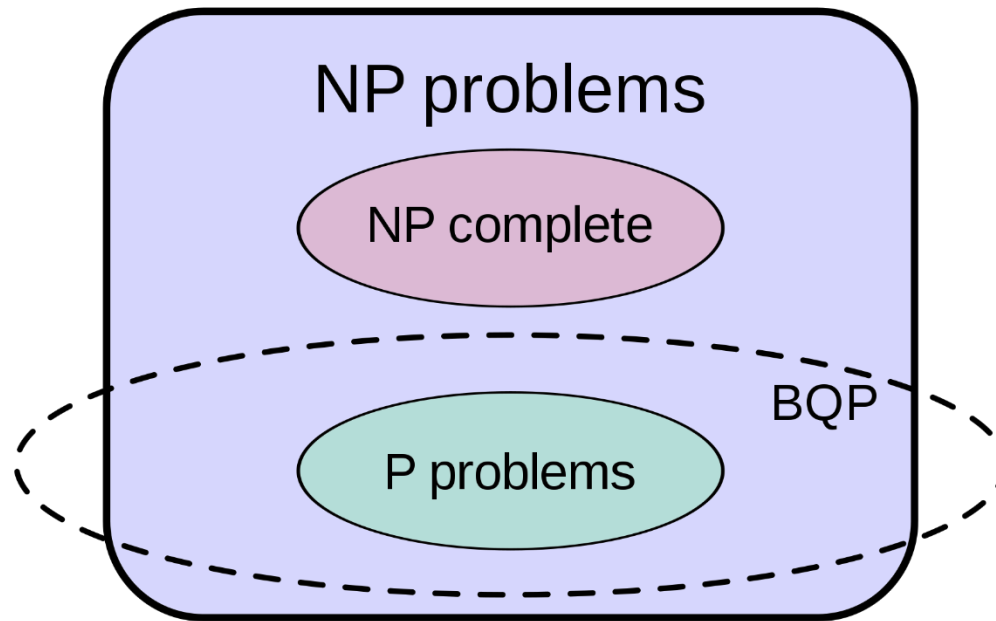



Image source:
Wikipedia

1. Are lattices/codes/isogenies/MQ in **BQP**? (Rebuild PQC)
 - **Hidden Subgroup Problem**: abelian (DL, factoring), dihedral (lattices)
2. Are factoring/DL/lattices/codes/isogenies/MQ/etc. in **P**? (Rebuild PKC)
3. Are **NP-complete** problems in **BQP**? (No PQC)
4. Is **P = NP**? (No Cryptography, except one-time pad)

Notable Failed Attempts

 Cornell University

We gratefully acknowledge support from the Simons Foundation, [member institutions](#), and all contributors. [Donate](#)

arXiv > quant-ph > arXiv:1611.06999

Search...
Help | Ad

Quantum Physics

This paper has been withdrawn by Lior Eldar

[Submitted on 21 Nov 2016 (v1), last revised 24 Nov 2016 (this version, v2)]

An Efficient Quantum Algorithm for a Variant of the Closest Lattice-Vector Problem

Lior Eldar, Peter W. Shor

The Systematic Normal Form (SysNF) is a canonical form of lattices introduced in [Eldar,Shor '16], in which the basis entries satisfy a certain co-primality condition. Using a "smooth" analysis of lattices by SysNF lattices we design a quantum algorithm that can efficiently solve the following variant of the bounded-distance-decoding problem: given a lattice L , a vector v , and numbers $b = \{\lambda_1(L)/n^{17}\}$, $a = \{\lambda_1(L)/n^{13}\}$ decide if v 's distance from L is in the range $[a/2, a]$ or at most b , where $\lambda_1(L)$ is the length of L 's shortest non-zero vector. Improving these parameters to $a = b = \{\lambda_1(L)/\sqrt{n}\}$ would invalidate one of the security assumptions of the Learning-with-Errors (LWE) cryptosystem against quantum attacks.

Comments: This paper has been withdrawn by the author due to an error in Fact 7: the concentration of measure of the n -dimensional sinc² function is not a probability of at least $1 - n^{-3}$ for vectors of length at most n^2 , but rather $1 - n^{-1.5}$ for vectors of length n^3

Subjects: Quantum Physics (quant-ph)

Cite as: arXiv:1611.06999 [quant-ph]
(or arXiv:1611.06999v2 [quant-ph] for this version)
<https://doi.org/10.48550/arXiv.1611.06999>

Submission history

From: Lior Eldar [[view email](#)]
[v1] Mon, 21 Nov 2016 20:33:06 UTC (252 KB)
[v2] Thu, 24 Nov 2016 12:57:42 UTC (1 KB) ([withdrawn](#))

Notable Failed Attempts



Cryptology ePrint Archive

Papers ▾ Submissions ▾ About ▾

Paper 2024/555

Quantum Algorithms for Lattice Problems

Yilei Chen , Tsinghua University, Shanghai Artificial Intelligence Laboratory, Shanghai Qi Zhi Institute

Abstract

We show a polynomial time quantum algorithm for solving the learning with errors problem (LWE) with certain polynomial modulus-noise ratios. Combining with the reductions from lattice problems to LWE shown by Regev [J.ACM 2009], we obtain polynomial time quantum algorithms for solving the decisional shortest vector problem (GapSVP) and the shortest independent vector problem (SIVP) for all n -dimensional lattices within approximation factors of $\tilde{\Omega}(n^{4.5})$. Previously, no polynomial or even subexponential time quantum algorithms were known for solving GapSVP or SIVP for all lattices within any polynomial approximation factors.

To develop a quantum algorithm for solving LWE, we mainly introduce two new techniques. First, we introduce Gaussian functions with complex variances in the design of quantum algorithms. In particular, we exploit the feature of the Karst wave in the discrete Fourier transform of complex Gaussian functions. Second, we use windowed quantum Fourier transform with complex Gaussian windows, which allows us to combine the information from both time and frequency domains. Using those techniques, we first convert the LWE instance into quantum states with purely imaginary Gaussian amplitudes, then convert purely imaginary Gaussian states into classical linear equations over the LWE secret and error terms, and finally solve the linear system of equations using Gaussian elimination. This gives a polynomial time quantum algorithm for solving LWE.

Note: Update on April 18: Step 9 of the algorithm contains a bug, which I don't know how to fix. See Section 3.5.9 (Page 37) for details. I sincerely thank Hongxun Wu and (independently) Thomas Vidick for finding the bug today. Now the claim of showing a polynomial time quantum algorithm for solving LWE with polynomial modulus-noise ratios does not hold. I leave the rest of the paper as it is (added a clarification of an operation in Step 8) as a hope that ideas like Complex Gaussian and windowed QFT may find other applications in quantum computation, or tackle LWE in other ways.

Metadata

Available format(s)



Publication info

Preprint.

Contact author(s)

chenyilei ra @ gmail com

History

2024-04-19: revised

2024-04-10: received

[See all versions](#)

Short URL

<https://ia.cr/2024/555>

License



CC BY