# MATHEMATICAL FRONTIERS

The National Academies of SCIENCES ENGINEERING MEDICINE

nas.edu/MathFrontiers

## Board on Mathematical Sciences & Analytics

# MATHEMATICAL FRONTIERS
## 2019 Monthly Webinar Series, 2-3pm ET

**February 12:** *Machine Learning for Materials Science**

**March 12:** *Mathematics of Privacy**

**April 9:** *Mathematics of Gravitational Waves**

**May 14:** *Algebraic Geometry**

**June 11:** *Mathematics of Transportation**

**July 9:** *Cryptography & Cybersecurity**

**August 13:** *Machine Learning in Medicine**

**September 10:** *Logic and Foundations**

**October 8:** *Mathematics of Quantum Physics**

**November 12:** *Quantum Encryption*

**December 10:** *Machine Learning for Text*

** Webinar posted*

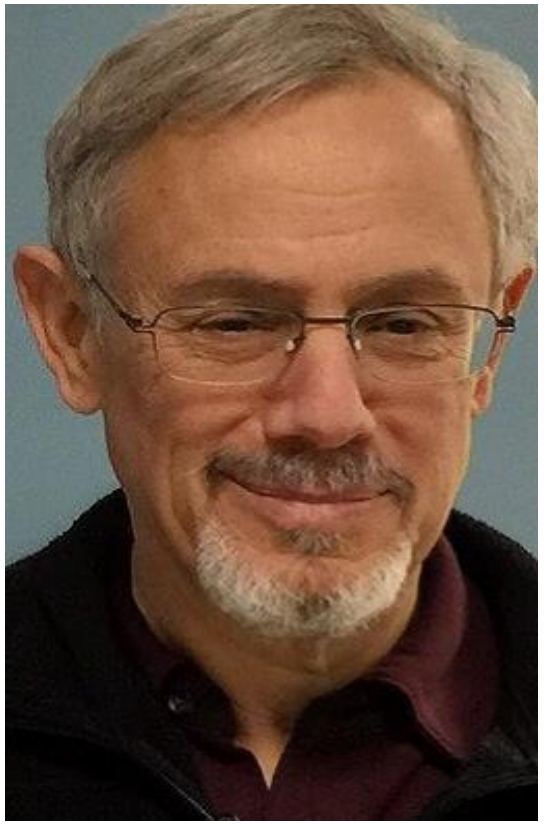
*Made possible by support for BMSA from the*
***National Science Foundation***
***Division of Mathematical Sciences***
*and the*
***Department of Energy***
***Advanced Scientific Computing Research***

*View webinar videos and learn more about BMSA at www.nas.edu/MathFrontiers*

# MATHEMATICAL FRONTIERS
## Quantum Encryption

**Delaram Kahrobaei,**
**University of York**

**Dustin Moody,**
**NIST**



**Mark Green,**
**UCLA (moderator)**

*View webinar videos and learn more about BMSA at www.nas.edu/MathFrontiers*

# MATHEMATICAL FRONTIERS
## Quantum Encryption

**Prof. Delaram Kahrobaei**
**University of York**

*Chair of Cyber Security University of York (UK)*
*Adjunct Professor of Computer Science*
*NYU: New York University*
*Doctoral Faculty of Computer Science GC*
*CUNY: The City University of New York*

# Post-Quantum Cryptography

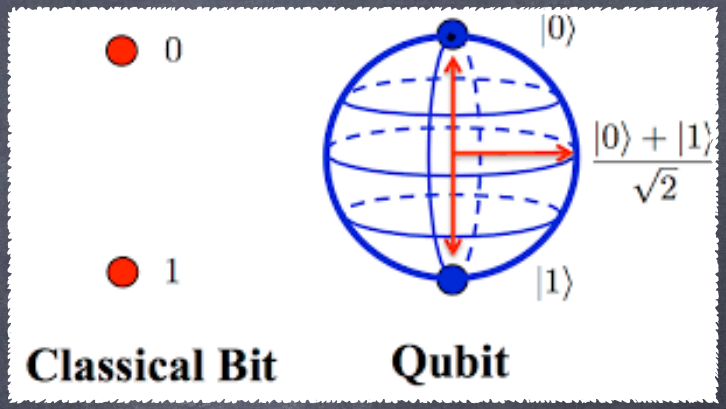
# Quantum Computation

- Quantum Computers are Not a replacement of the classical computers
- It works faster for some special classes of problems.

# qubit

- A qubit is the quantum analogue of a classical bit, and can be thought of as vectors. The basis states (basis vectors) are

$$|0\rangle = \begin{matrix} 1 \\ [0] \end{matrix} \quad \text{and} \quad |1\rangle = \begin{matrix} 0 \\ [1] \end{matrix}$$

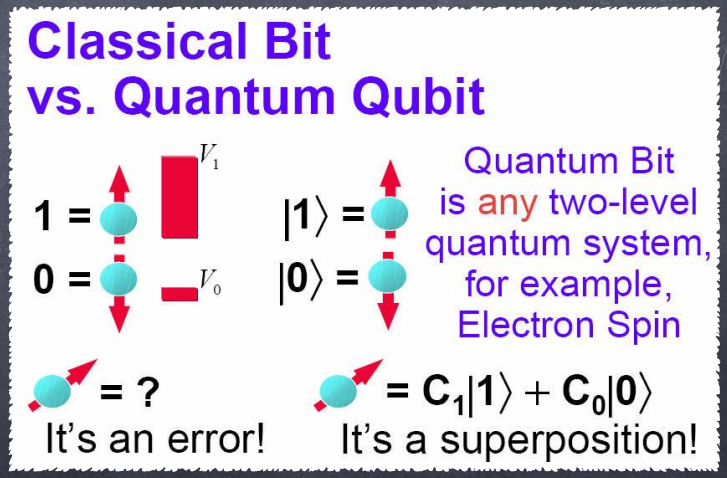


# Combined cubits

- These can be combined. If we have two qubits, the states are

$$|00\rangle = \begin{bmatrix}1\\0\\0\\0\end{bmatrix} \quad |01\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}$$

$$|10\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix} \quad |11\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

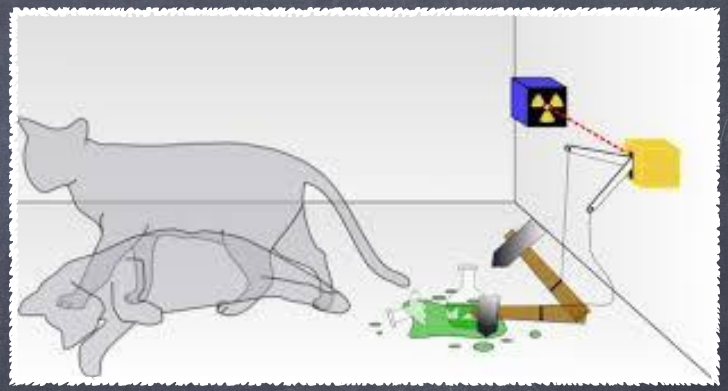


# Superposition

- A pure qubit state is a linear superposition of these basis states, with probability amplitudes

$$\alpha, \beta \in \mathbb{C}$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$



# How many qubits do we have?

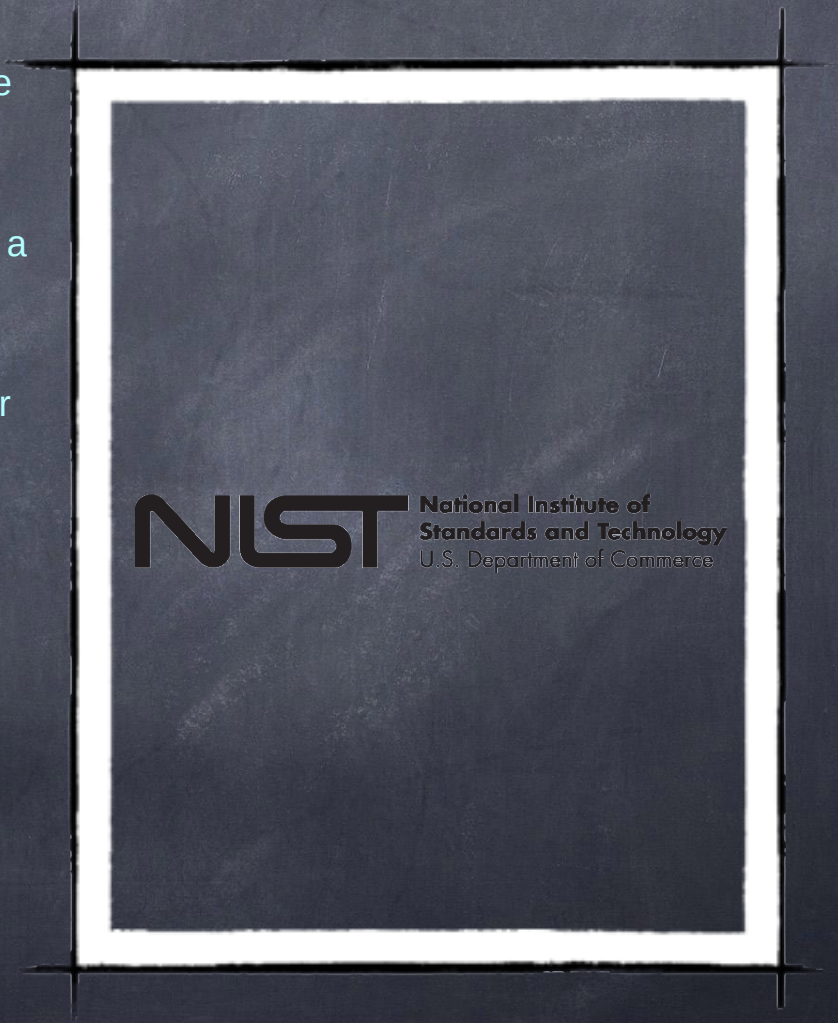
- A pair of qubits that can exist as either 1s or 0s can embody 4 possible states.
- 3 qubits can embody 8.

# NSA NIST

- Announcement for Search of Post-Quantum Primitives

# The quantum-safe primitives under consideration by NIST

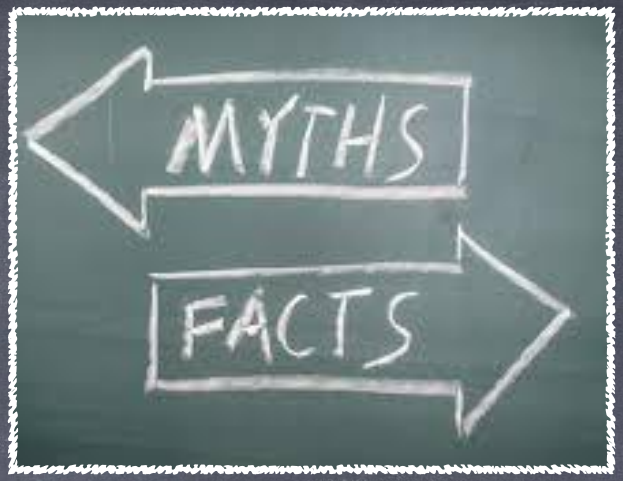
- Multivariate primitives (System of multivariate polynomial equations)
- Code-based primitives (Decoding problem in a linear code)
- Lattice-based primitives (Short or close vector problem in a lattice)
- Hash-based primitives (Finding collisions or preimages in cryptographic hash functions)
- Isogeny-based key primitives (finding an unknown isogeny between a pair of supersingular elliptic curves)
- Group-based primitives (algorithmic group theoretic problems)



# Cyber Security: Cryptography

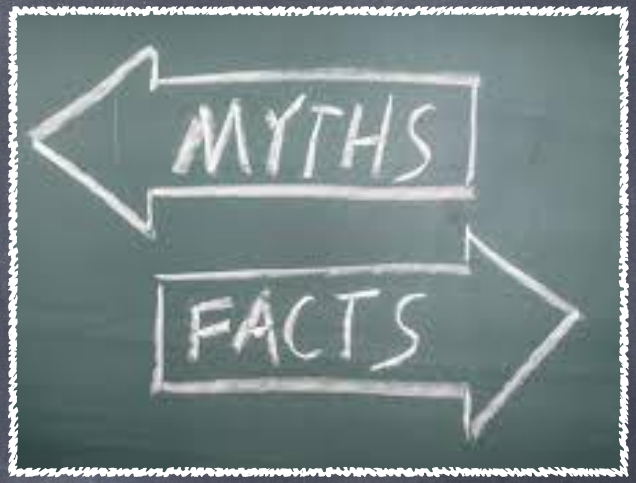
- Key Exchanges (RSA, DH)
- Symmetric Key Encryption
- Digital Signatures
- Multilinear Maps
- Fully Homomorphic Encryptions
- Authentication
- Secret Sharing

# Group Theory in Cryptography




- Polycyclic Groups: Eick, Kahrobaei
- Graph (RAAG) Groups: Flores, Kahrobaei, Koberda
- Hyperbolic Groups: Chatterji, Kahrobaei
- Arithmetic Groups: Kahrobaei, Mallahi-Karai
- Nilpotent Groups: Kahrobaei, Tortora, Tota
- Engel Groups: Kahrobaei, Noce
- Free nilpotent p-groups: Kahrobaei, Shpilrain
- Semigroup of Matrices over Group-Rings: Kahrobaei, Koupparis, Shpilrain
- Small Cancellation Groups: Habeeb, Kahrobaei, Shpilrain
- Free Metabelian: Groups: Shpilrain, Zapata, , Kahrobaei, Habeeb

# Group Theory in Cryptography




- Linear: Groups: Baumslag, Fine, Xu
- Braid Groups: Anshel-Anshel-Goldfeld, Ko-Lee
- Grigorchuk Groups: Petrides
- Automata Groups: Grigorchuk, Grigoriev
- Groups of Matrices: Grigoriev, Ponameranco
- Thompson: Groups: Shpilrain, Ushakov

# Algorithmic Group Theoretic Problems used in Cryptography

- Discrete Logarithm Problem
- Subgroup Isomorphism Problem
- Group Homomorphism Problem
- Power Conjugacy Search Problem
- Geodesic Length Problem
- Distorted Subgroup
- Conjugacy Search Problem
- Word Decision Problem
- Endomorphism Search Problem
- Decomposition Search Problem
- Subgroup membership Problem

# Approaches to Post-quantum Group-Based Cryptography

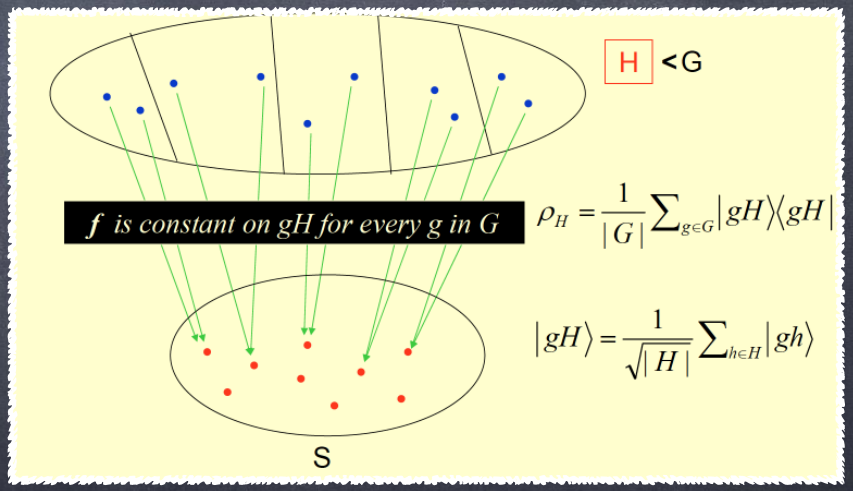
- NP-Complete and Unsolvable Group-Theoretic Problems
- Analysing equivalence to Hidden Subgroup Problem
- Analysing Grover's Search Problem

# Hidden Subgroup Problem (HSP)

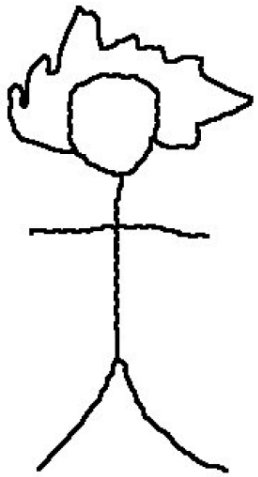
- Given a finitely generated group G and an efficiently computable function f from G to some finite set S such that f is constant and distinct on left-cosets of a subgroup H of finite index, find a generating set for H.

- Superposition

$$|G\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle$$

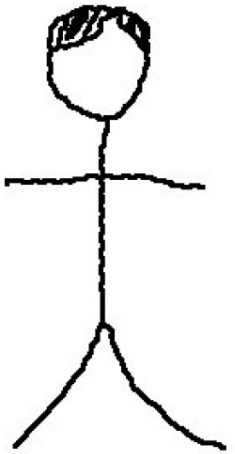


# Public Key-exchange Using Semidirect Products of (semi)Groups

Public: $G$, $g \in G$, $\phi$.

$a$, $b$



$(b, x) \cdot (a,\ \phi^m) =$

$(a,\ y) \cdot (b,\ \phi^n) =$

$(g,\ \phi)^{m+n}$

Private key: $m \in \mathbb{N}$

$(g, \phi)^m =$

$(\underbrace{\phi^{m-1}(g) \cdots \phi^2(g) \cdot \phi(g) \cdot g}_{a},\ \phi^m)$

Private key: $n \in \mathbb{N}$

$b$

# Public Key-exchange Using Semidirect Products of (semi-)Groups

- DH is a special case of this protocol ($G = \mathbb{Z}_p{}^*$).
- Using Free Nilpotent $p$-groups.

Can we show this scheme is post-quantum: Analysing the HSP for Free Nilpotent $p$-groups and also the underlying security assumption?!

M. Habeeb, D. Kahrobaei, C. Koupparis, and V. Shpilrain, *Public key exchange using semidirect product of (semi)groups*, in: ACNS 2013, Applied Cryptography and Network Security **7954** (2013), 475–486.

D. Kahrobaei, V. Shpilrain, *Invited Paper: Using semidirect product of (semi)groups in public key cryptography*, Computability in Europe 2016, LNCS **9709**,132–141 (2016).

# Announcement

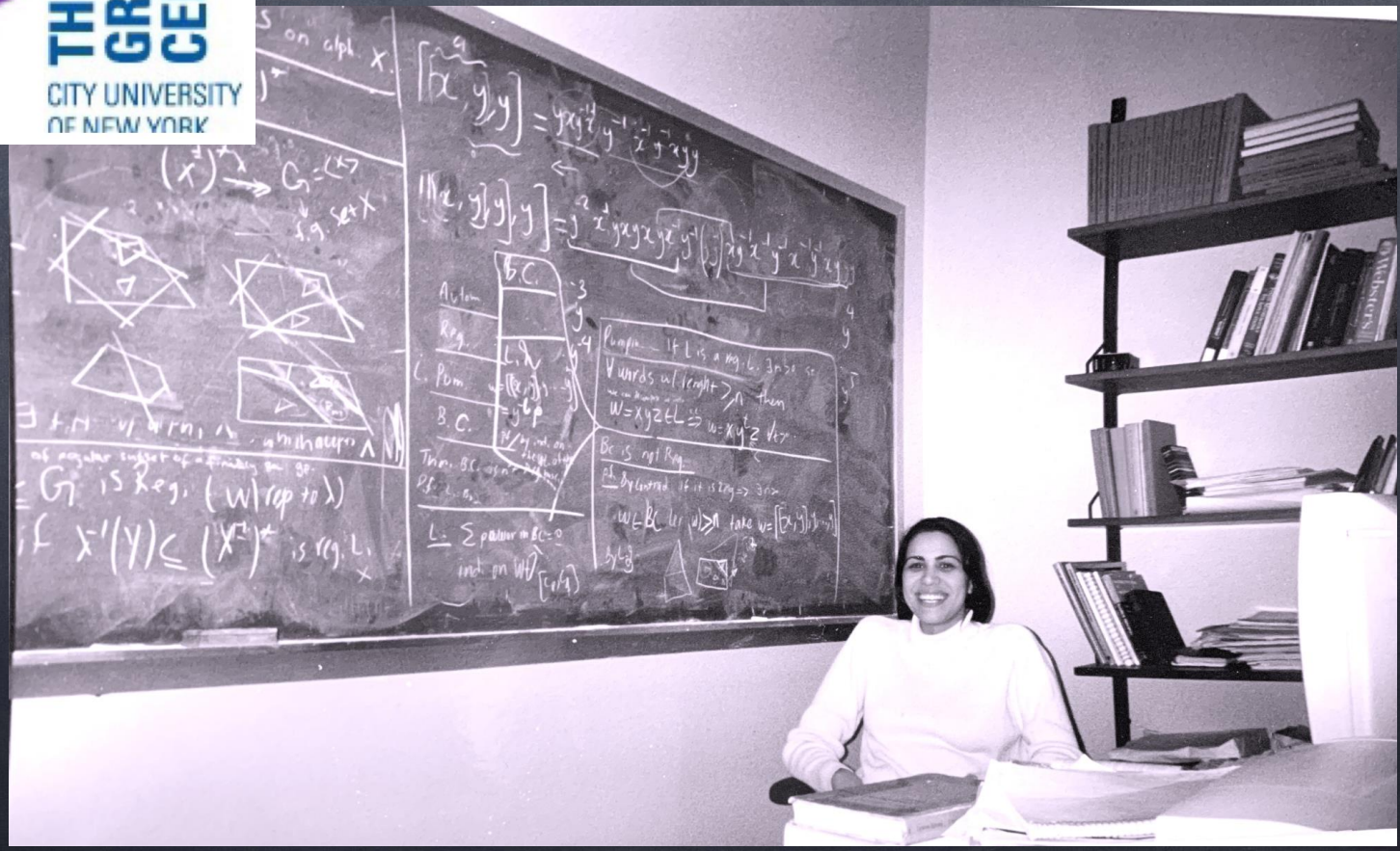
- Post-Quantum Algebraic Cryptography, Institut Henri Poincare, IHP, Paris, France, September-December 2021. [J-C. Faugère, D. Kahrobaei, L. Perret, V. Shpilrain]

UNIVERSITY of York

NYU

THE GRADUATE CENTER
CITY UNIVERSITY OF NEW YORK

# Thank you!



# MATHEMATICAL FRONTIERS
## Quantum Encryption

**Dustin Moody,**
**NIST**

*Mathematician*
*Cryptographic Technology Group*
*National Institute of Standards and Technology*

# Cryptography in a Post-Quantum World

# Quantum Computers

Google AI Blog

The latest news from Google AI

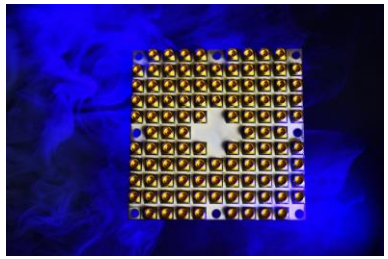
Quantum Supremacy Using a Programmable Superconducting Processor

Wednesday, October 23, 2019

Posted by John Martinis, Chief Scientist Quantum Hardware and Sergio Boixo, Chief Scientist Quantum Computing Theory, Google AI Quantum


Google's 72-qubit chip "Bristlecone"

IBM's 50-qubit quantum computer



Intel's 49-qubit chip "Tangle-Lake"

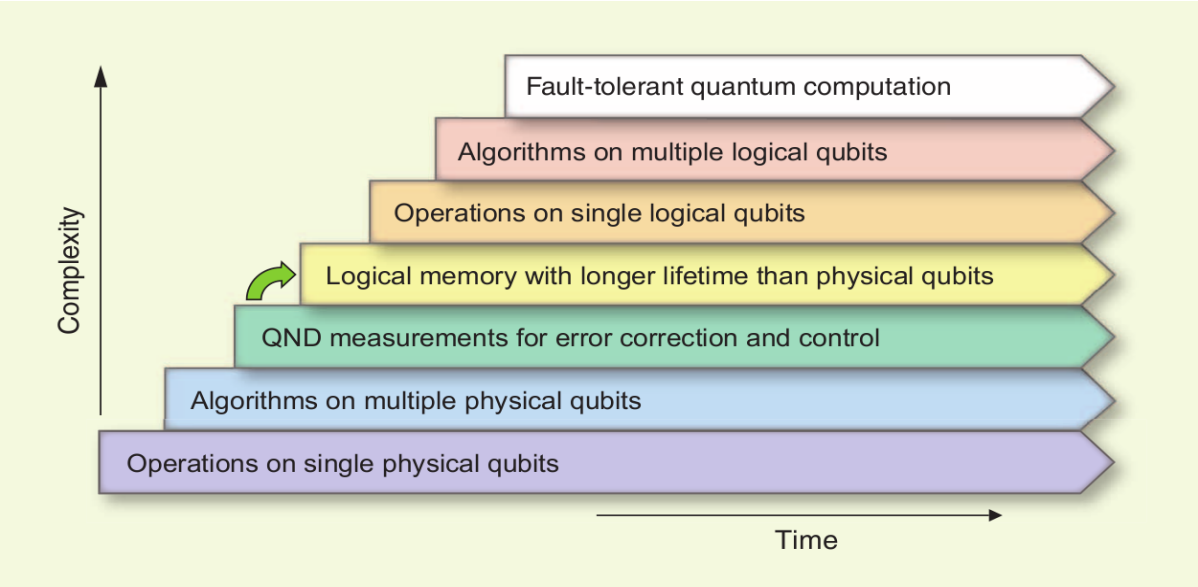
IBM

IBM Research Blog Topics Labs About


October 21, 2019 | Written by: Edwin Pednault, John Gunnels & Dmitri Maslov, and Jay Gambetta

# Quantum Computing Progress

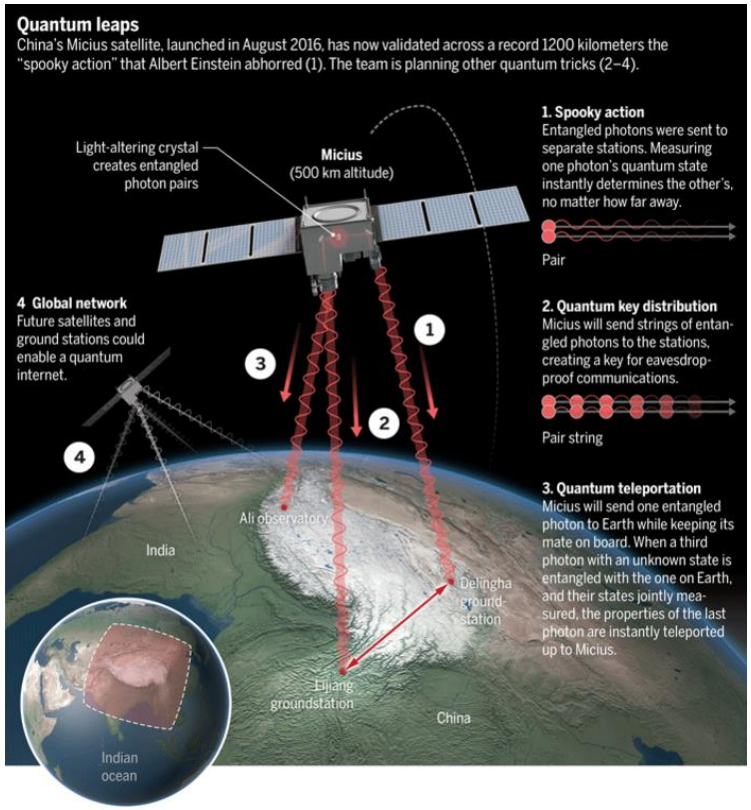
- A lot of progress, but still a long way to go




[Image credit: M. Devoret and R. Schoelkopf]

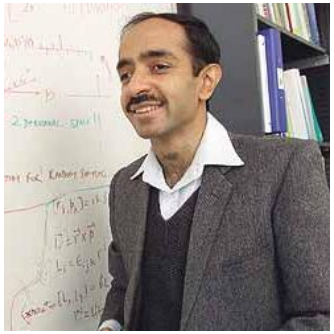
# Quantum Cryptography

- Using quantum technology to build cryptosystems
  - Theoretically unconditional security guaranteed by the laws of physics
- Limitations
  - Can do encryption, but not authentication
  - Quantum networks not very scalable
  - Expensive and needs special hardware
- Lots of money being spent on "quantum"

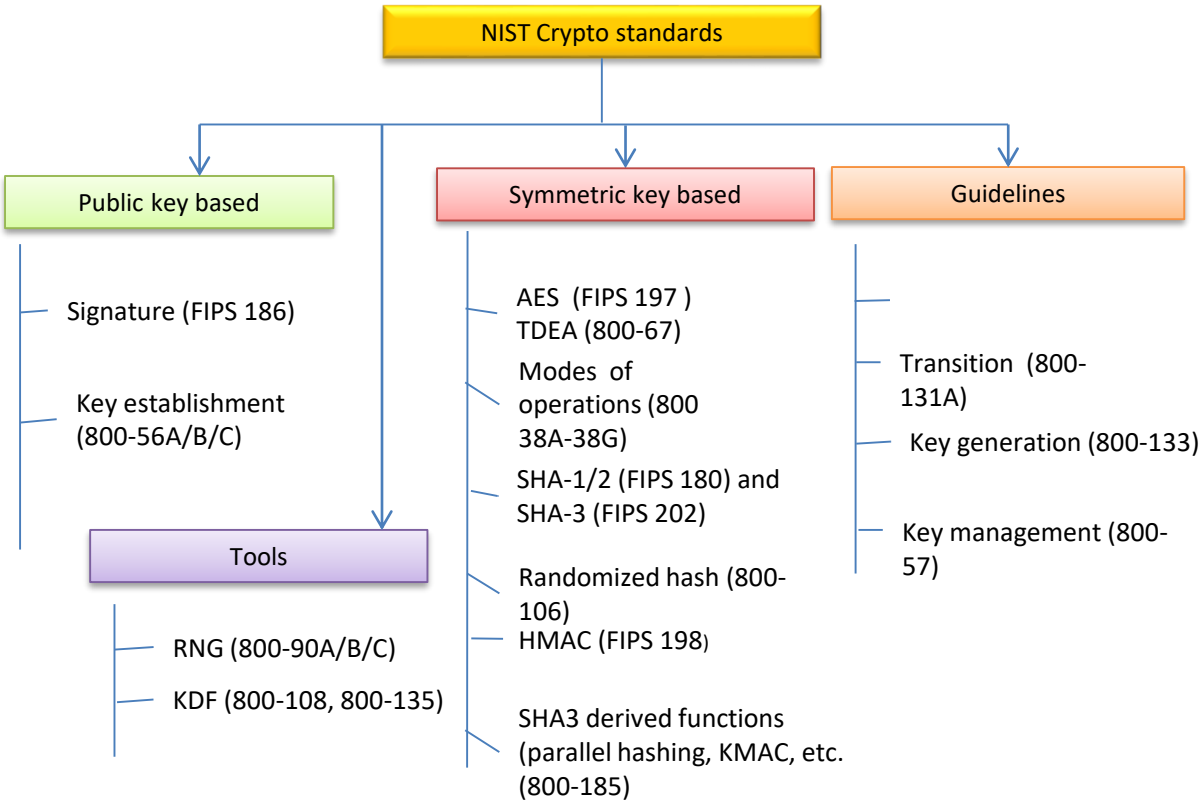


# Quantum Algorithms

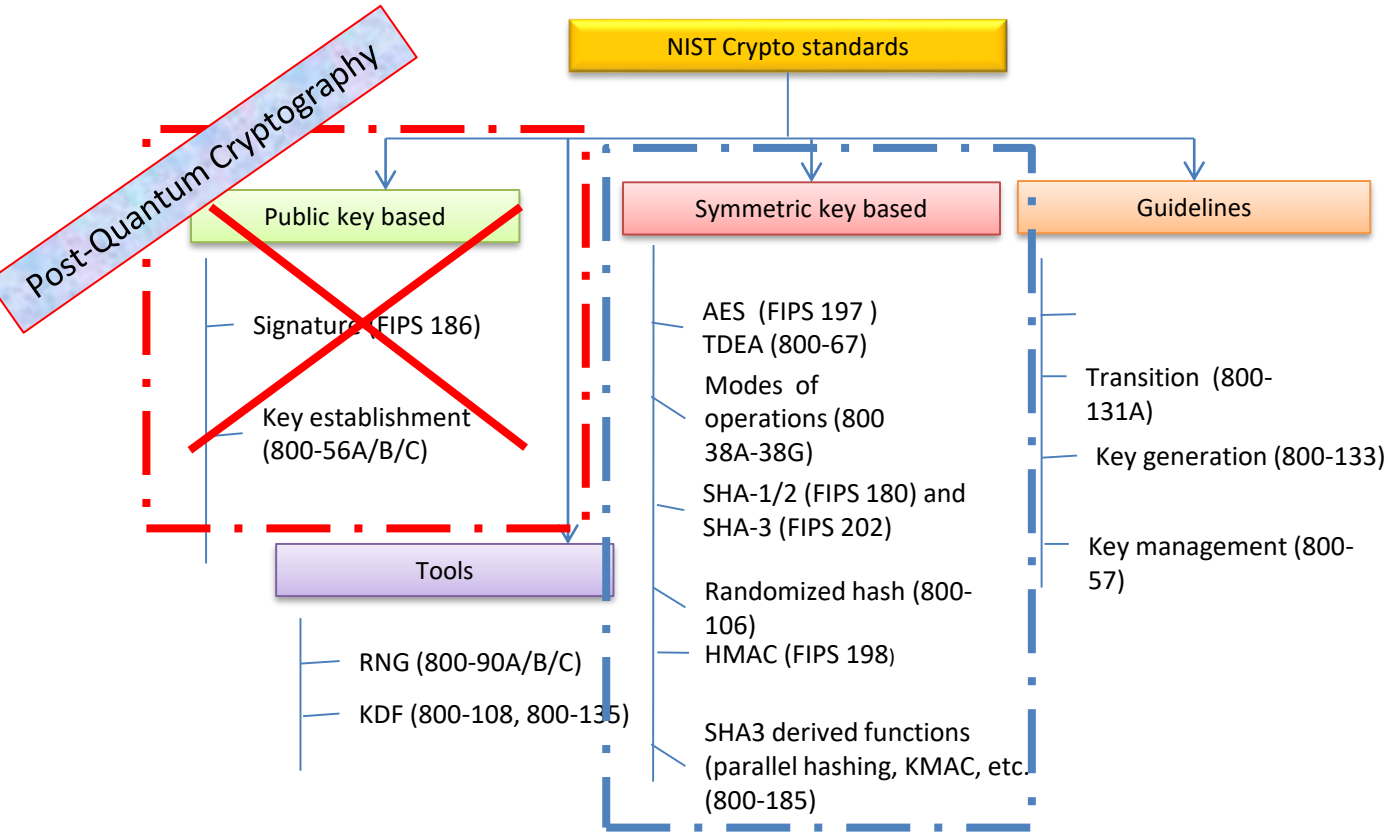
- 1994, Peter Shor created a quantum algorithm that would give an exponential speed-up over classical computers
  - Factoring large integers
  - Finding discrete logarithms
- Grover's algorithm – polynomial speed-up in unstructured search, from O($N$) to O($\sqrt{N}$)
- Simulating the dynamics of molecules, superconductors, photosynthesis, among many, many others
  - see http://math.nist.gov/quantum/zoo



# The Sky is Falling?




# The Sky is Falling?




# When will a Quantum Computer be Built?

- Quantum computers are 20 years in the future and always will be

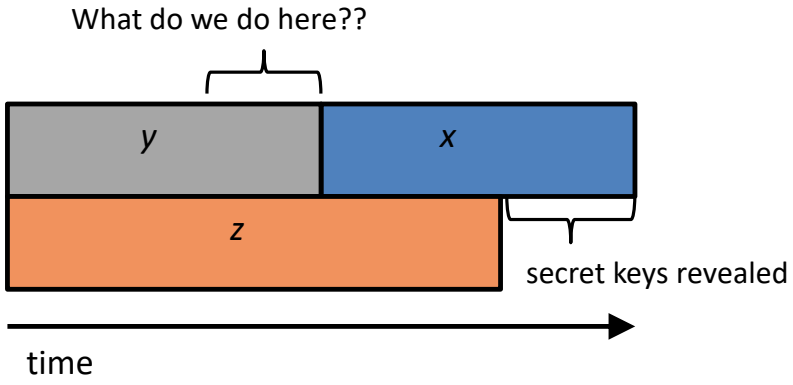
**"There is a 1 in 7 chance that some fundamental public-key crypto will be broken by quantum by 2026, and a 1 in 2 chance of the same by 2031."**

– Dr. Michele Mosca, U. of Waterloo (2016)

# How soon do we need to worry?

- How long does your information need to be secure (*x* years)
- How long to re-tool existing infrastructure with quantum safe solution (*y* years)
- How long until large-scale quantum computer is built (*z* years)

Theorem (Mosca): If $x + y > z$, then worry

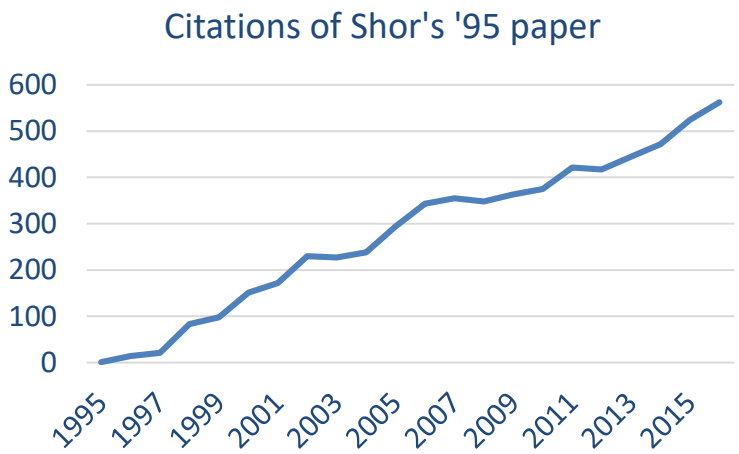


# Post-Quantum Cryptography (PQC)

- Cryptosystems which run on classical computers, and are considered to be resistant to quantum attacks

- PQC needs time to be ready for applications
  - Efficiency
  - Confidence – cryptanalysis
  - Standardization
  - Usability and interoperability

  (IKE, TLS, etc… use public key crypto)



# NIST's PQC Project

- NIST is running a worldwide "competition" to select quantum-resistant algorithms for standardization
  - Open and transparent process
- Scope
  - Digital signatures (FIPS 186)
  - (Public-key) Encryption (SP 800-56B) /Key-establishment (KEMs) (SP 800-56A)
- Expected outcome: a few different algorithms

# Evaluation Criteria

- Security – against both classical and quantum attacks

| Level | Security Description |
|---|---|
| I | At least as hard to break as AES128 (exhaustive key search) |
| II | At least as hard to break as SHA256 (collision search) |
| III | At least as hard to break as AES192 (exhaustive key search) |
| IV | At least as hard to break as SHA384 (collision search) |
| V | At least as hard to break as AES256 (exhaustive key search) |

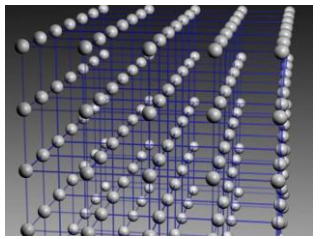
  - NIST asked submitters to focus on levels 1,2, and 3
- Performance – measured on various classical platforms
- Other properties:
  - Drop-in replacements, Perfect forward secrecy, Resistance to side-channel attacks, Simplicity and flexibility, Misuse resistance, etc…

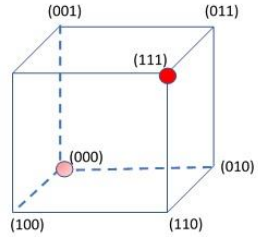
# The 1st Round Candidates

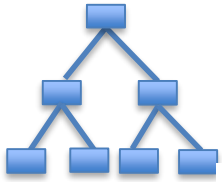
- Nov 2017 - 82 submissions received.
- 69 accepted as “complete and proper” (5 withdrew)

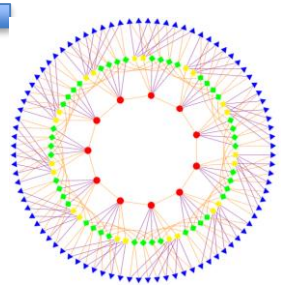
$$p^{(1)}(x_1,\ldots,x_n)=\sum_{i=1}^{n}\sum_{j=i}^{n}p_{ij}^{(1)}\cdot x_i x_j \;+\; \sum_{i=1}^{n}p_i^{(1)}\cdot x_i + p_0^{(1)}$$
$$p^{(2)}(x_1,\ldots,x_n)=\sum_{i=1}^{n}\sum_{j=i}^{n}p_{ij}^{(2)}\cdot x_i x_j \;+\; \sum_{i=1}^{n}p_i^{(2)}\cdot x_i + p_0^{(2)}$$
$$\vdots$$
$$p^{(m)}(x_1,\ldots,x_n)=\sum_{i=1}^{n}\sum_{j=i}^{n}p_{ij}^{(m)}\cdot x_i x_j \;+\; \sum_{i=1}^{n}p_i^{(m)}\cdot x_i + p_0^{(m)}$$

| | Signatures | KEM/Encryption | Overall |
|---|---|---|---|
| Lattice-based | 5 | 21 | 26 |
| Code-based | 2 | 17 | 19 |
| Multi-variate | 7 | 2 | 9 |
| Symmetric-based | 3 | | 3 |
| Other | 2 | 5 | 7 |
| | | | |
| Total | **19** | **45** | **64** |







*View webinar videos and learn more about BMSA at www.nas.edu/MathFrontiers*

# 25 Countries, 16 States, 6 Continents


*View webinar videos and learn more about BMSA at www.nas.edu/MathFrontiers*

# Overview of the 1st Round

- Began Dec 2017 – 1st Round Candidates published
- Resources:
  - Internal and external cryptanalysis
  - The 1st NIST PQC Standardization
  - Research publications
  - Performance benchmarks
  - Official comments
  - The pqc-forum mailing list

- Ended Jan 30, 2019 – 2nd Round Candidates Announced

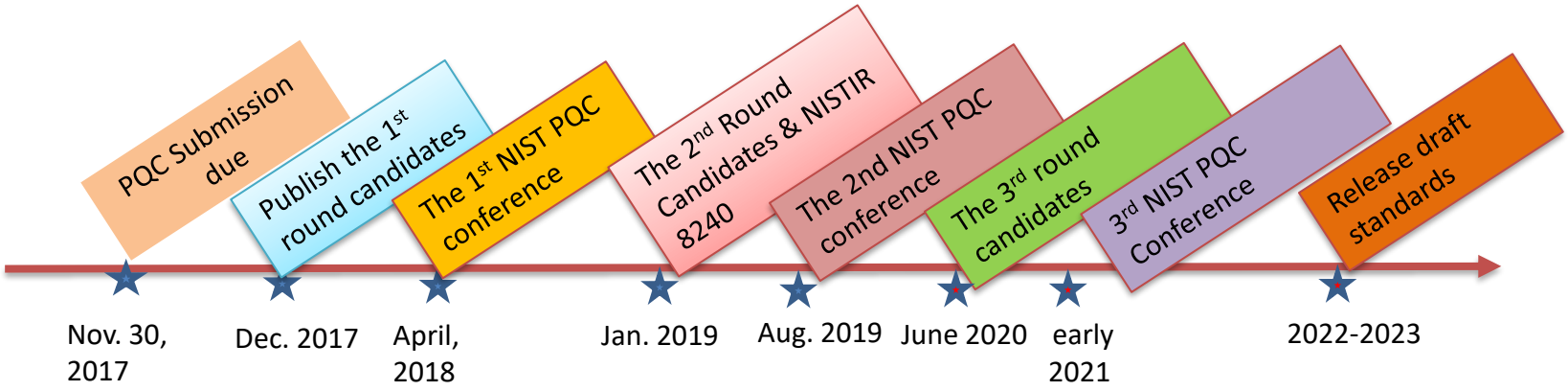
# The 2nd Round Candidates

- We wanted to keep algorithm diversity and promote research, but had to reduce the number of candidates to a manageable size for the community
  - It is often very difficult to compare candidates – even in the same family
  - Some submissions were merged together

| | Signatures | KEM/Encryption | Overall |
|---|---|---|---|
| Lattice-based | 3 | 9 | 12 |
| Code-based | | 7 | 7 |
| Multi-variate | 4 | | 4 |
| Symmetric based | 2 | | 2 |
| Isogeny | | 1 | 1 |
| Total | **9** | **17** | **26** |

# Timeline

- 12-18 months to analyze and evaluate the 2nd round candidates
- NIST will announce the 3rd round candidates around June 2020
- The 3rd NIST PQC Standardization Conference will be in early 2021
- Release draft standards in 2022-2023 for public comments



# What can your organization do NOW?

- Perform a quantum risk assessment within your organization
  - Identify information assets and their current crypto protection
  - Identify what ‘x’, ‘y’, and ‘z’ might be for you – determine your quantum risk
  - Prioritize activities required to maintain awareness, and to migrate technology to quantum-safe solutions
- Evaluate vendor products with quantum safe features
  - Know which products are not quantum safe
  - Ask vendors for quantum safe features in procurement templates
- Develop an internal knowledge base amongst IT staff
- Track developments in quantum computing and quantum safe solutions, and to establish a roadmap to quantum readiness for your organization

- Act now – it will be less expensive, less disruptive, and less likely to have mistakes caused by rushing and scrambling

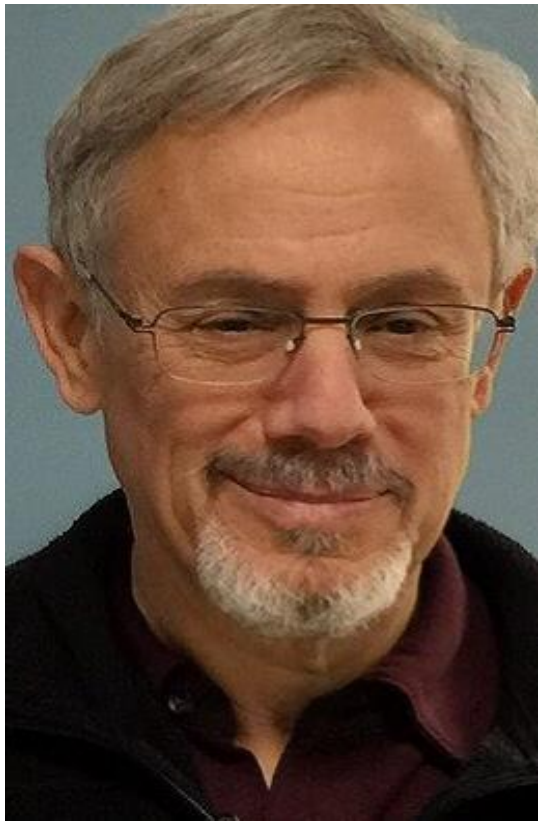
# Summary

- Quantum computers have HUGE potential
- Post-quantum crypto standardization will be a long journey
- Check out www.nist.gov/pqcrypto
  - Sign up for the pqc-forum for announcements & discussion

# MATHEMATICAL FRONTIERS
## Quantum Encryption

**Delaram Kahrobaei,**
**University of York**

**Dustin Moody,**
**NIST**



**Mark Green,**
**UCLA (moderator)**

*View webinar videos and learn more about BMSA at www.nas.edu/MathFrontiers*

# MATHEMATICAL FRONTIERS
## 2019 Monthly Webinar Series, 2-3pm ET

**February 12:** *Machine Learning for Materials Science**

**March 12:** *Mathematics of Privacy**

**April 9:** *Mathematics of Gravitational Waves**

**May 14:** *Algebraic Geometry**

**June 11:** *Mathematics of Transportation**

**July 9:** *Cryptography & Cybersecurity**

**August 13:** *Machine Learning in Medicine**

**September 10:** *Logic and Foundations**

**October 8:** *Mathematics of Quantum Physics**

**November 12:** *Quantum Encryption*

**December 10:** *Machine Learning for Text*

** Webinar posted*

*Made possible by support for BMSA from the*
***National Science Foundation***
***Division of Mathematical Sciences***
*and the*
***Department of Energy***
***Advanced Scientific Computing Research***

*View webinar videos and learn more about BMSA at www.nas.edu/MathFrontiers*