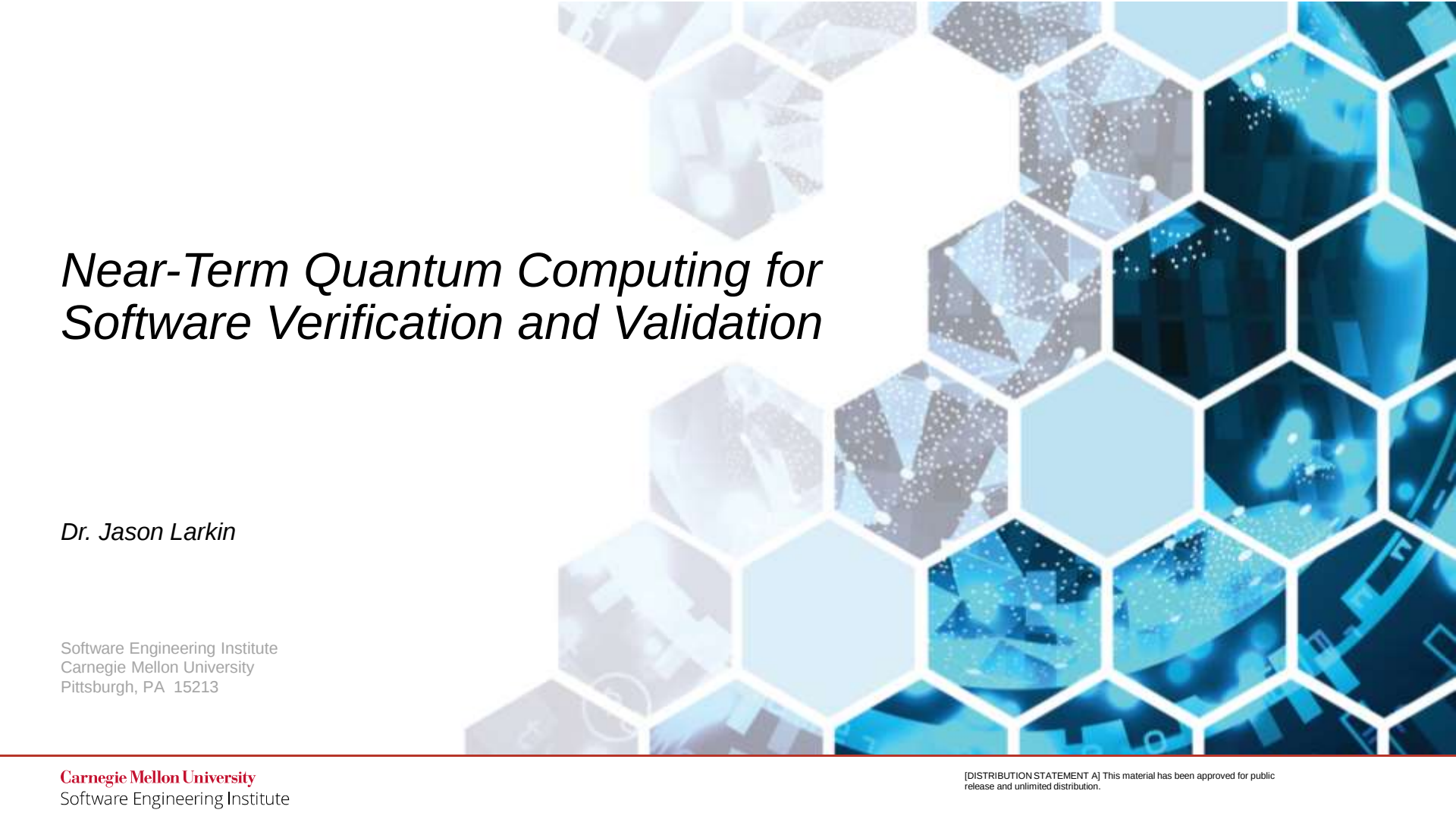




Near-Term Quantum Computing for Software Verification and Validation

Dr. Jason Larkin

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Legal

Copyright 2018 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material was prepared for the exclusive use of Washington, D.C. Quantum Meetup and may not be used for any other purpose without the written consent of permission@sei.cmu.edu.

Carnegie Mellon® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM18-1271

Dr. Jason Larkin



Research Scientist

CMU SEI,
Emerging Technology Center
Software VV and Advanced Computing

Why SEI? Software verification and validation (VV)

- Software VV is a core SEI mission (and for any Software Engineer).
- Alignment with ETC technical area: We are applying advanced computing to this core mission.
- Focus on the software engineering challenges

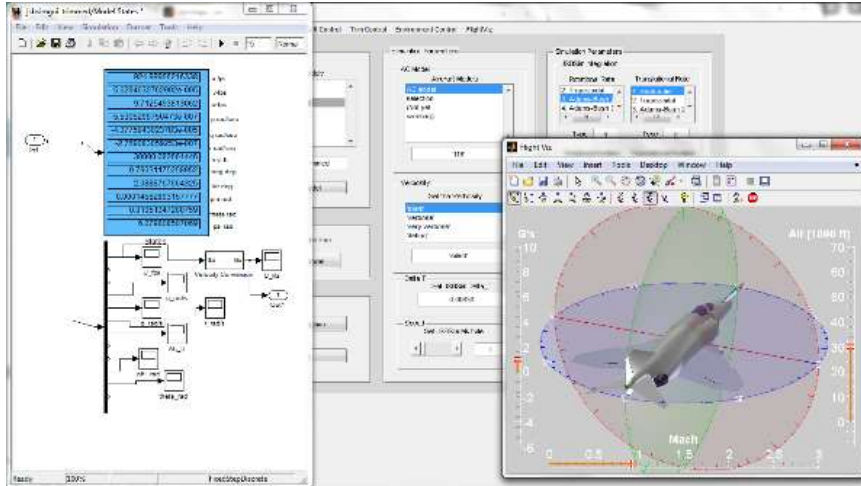
If successful...will have made a significant contribution to...



Why is Software VV important (and HARD) for DoD?

“...on average, half the **cost** of creating [complex software] is on **VV**.”

— C. Elliott, Safe & Secure Systems & Software Symposium 2016.

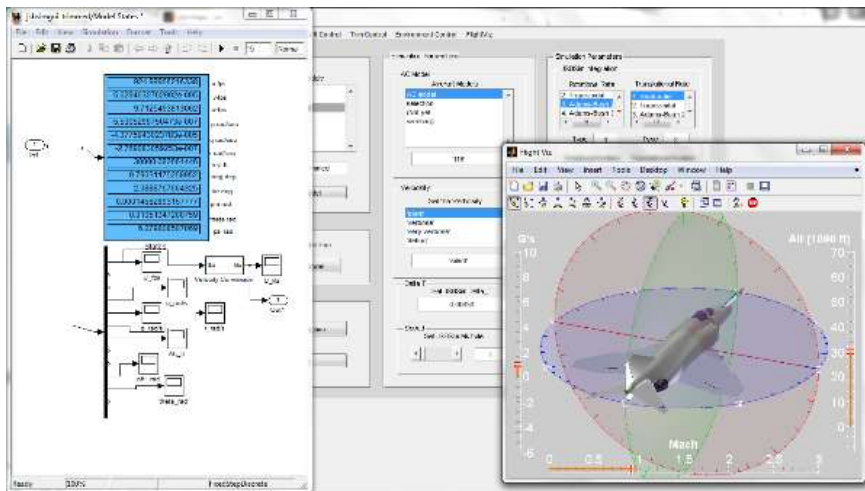


github.com/esp8266/Arduino

Why is Software VV important (and HARD) for DoD?

“...on average, half the **cost** of creating [complex software] is on **VV**.”

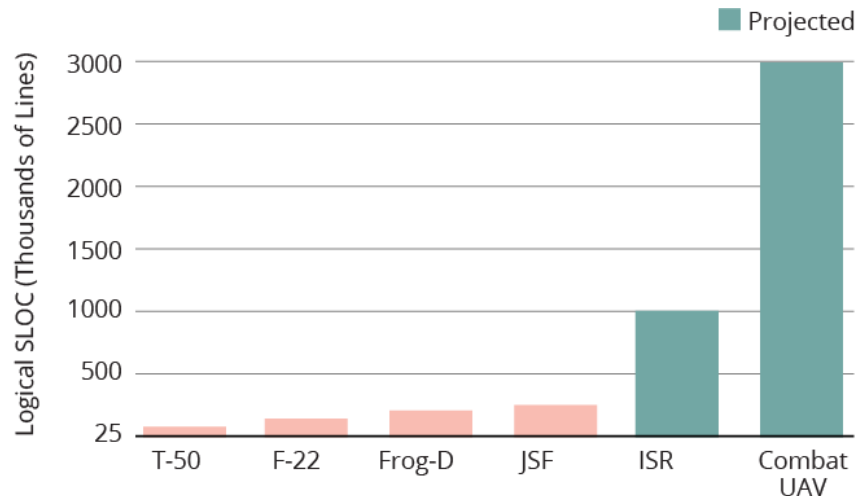
— C. Elliott, Safe & Secure Systems & Software Symposium 2016.



Software VV Tools

Computational Cost ~ exp(size)
100-1 millions years

And this cost is increasing...



“next generation Software VV will require new computing paradigm...”

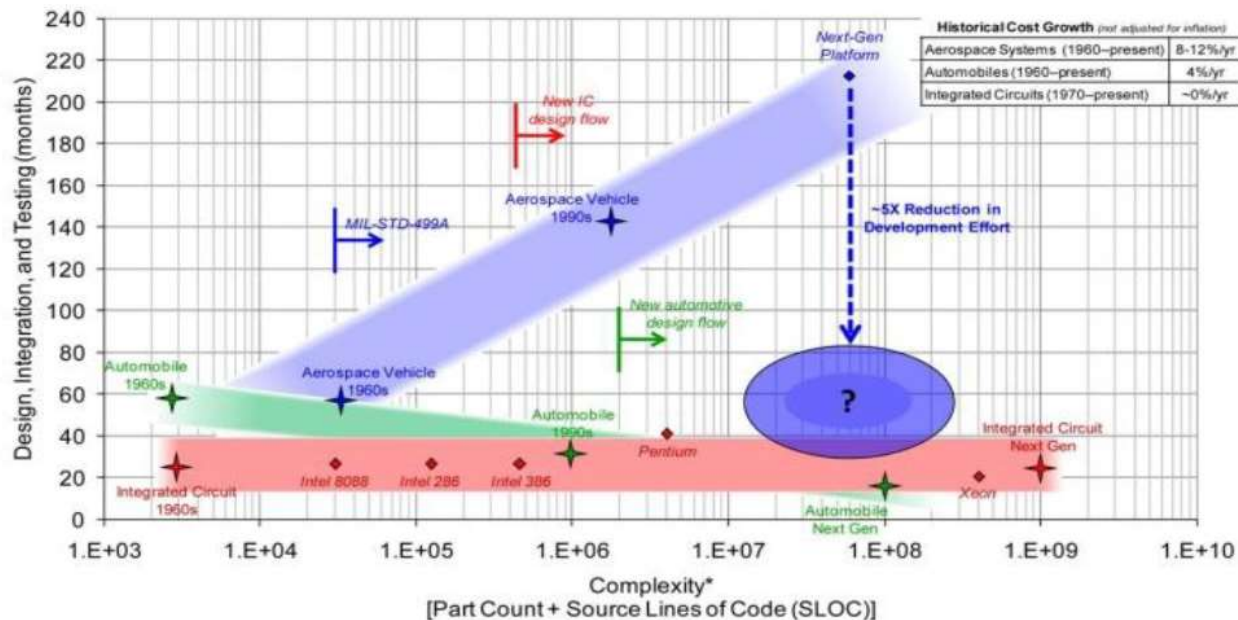
T. Belote, C. Elliott, Safe & Secure Systems & Software Symposium 2014.

Software VV Challenges

APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED.

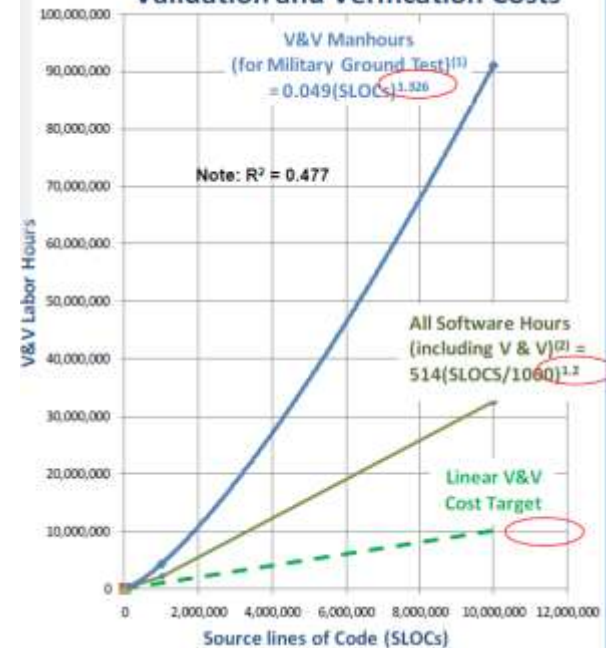


Historical schedule trends with complexity

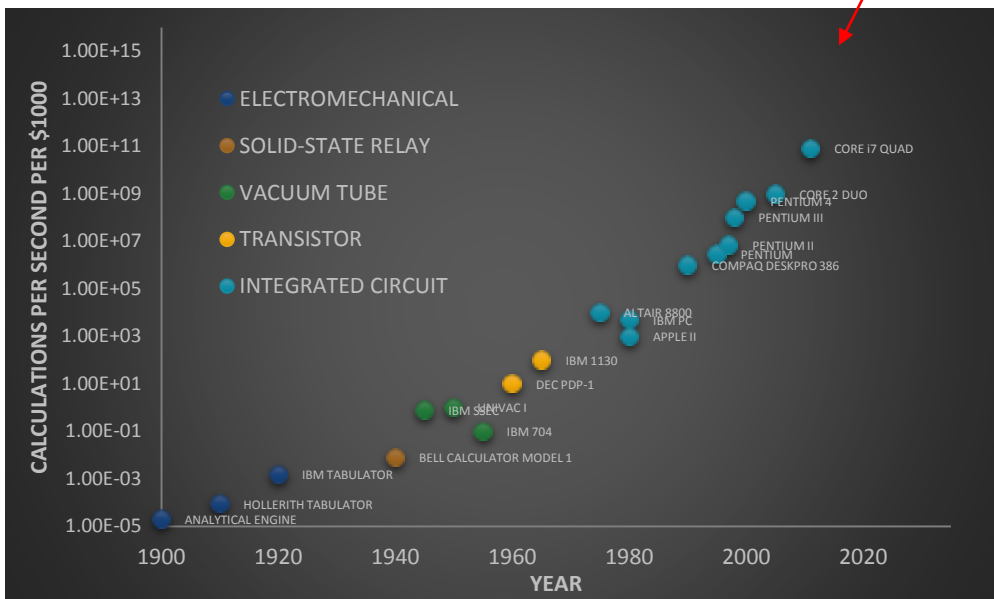


Note (*): Not a great metric. But that's what we have today. META will come up with better metrics.

Validation and Verification Costs



Is Quantum Computing the next major Paradigm?



H.R.5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019

115th Congress (2017-2018) | [Get alerts](#)

SEC. 234. DEFENSE QUANTUM INFORMATION SCIENCE AND TECHNOLOGY RESEARCH AND DEVELOPMENT PROGRAM.

IN THE SENATE OF THE UNITED STATES A BILL

To require the Secretary of Defense to establish the Defense Quantum Information Consortium, and for other purposes.

Quantum Computing Applications with State of the Art Capabilities Request for Information (RFI)

Solicitation Number: DARPA-SN-18-68

Agency: Other Defense Agencies

Office: Defense Advanced Research Projects Agency

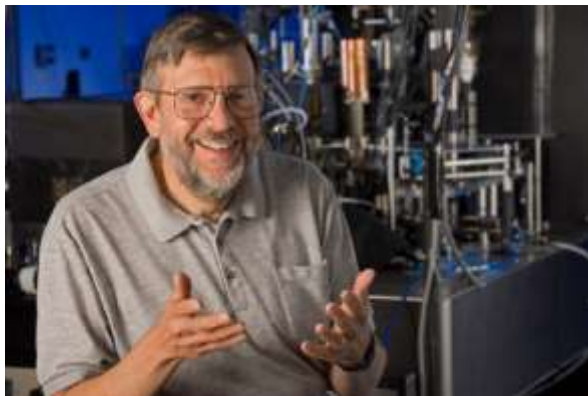
<https://www.congress.gov/bill/115th-congress/senate-bill/2987/>

<https://www.harris.senate.gov/news/press-releases/harris-introduces-bill-to-increase-resources-for-quantum-computing-and-research-to-benefit-national-security>

<https://www.fbo.gov/spg/ODA/DARPA/CMO/DARPA-SN-18-68/listing.html>

What is Quantum Computing?

Bill Phillips
NIST/JQI



“A Quantum Computer differs more from a classical computer...than a classical computer differs from an ABACUS”

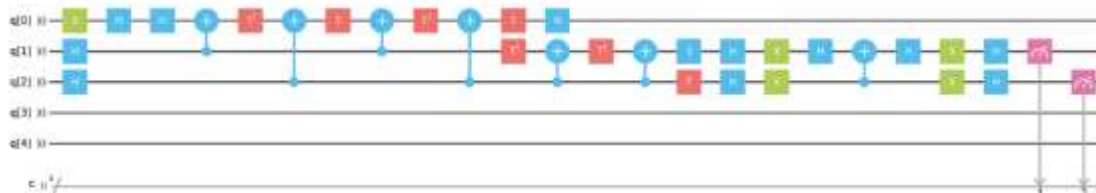
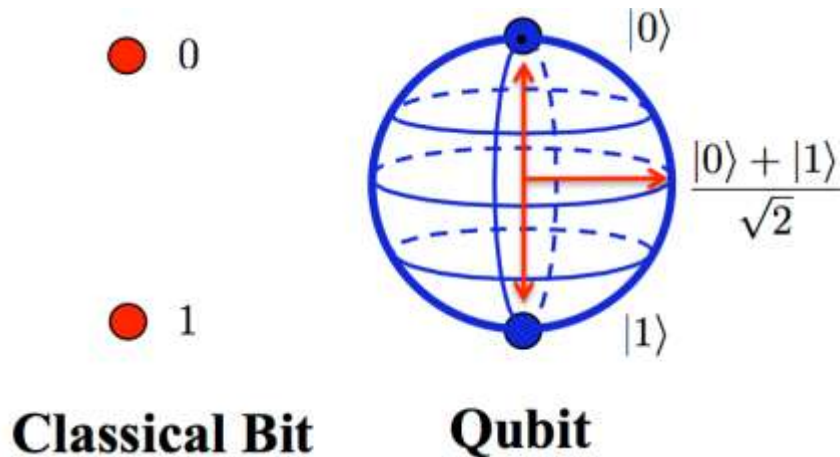


FIG. 2: The circuit that was executed on IBM's 5-qubit quantum computer (ibmqx4 was used). The first two time slots correspond to the state preparation. The next 13 time slots implement a Toffoli gate. The next 7 time slots implement the $2|\psi\rangle\langle\psi| - I$ operator, and the final two time slots are used for observing x_1 and x_2 .

Why is it important to DoD?

Science Home News Journals Topics Careers

Update: Quantum physics gets attention—and brighter funding prospects—in Congress

By Gabriel Popkin | Jan. 27, 2018, 12:50 PM

Many members of Congress admit they find quantum physics mind-boggling, with its counterintuitive account of the subatomic world. But that isn't stopping U.S. lawmakers, as well as policymakers in President Donald Trump's administration, from backing an ambitious effort to better recognize and fund quantum computing.

INTELLIGENCE COMMUNITY

Your source for breaking news from across the intelligence community contracting landscape. Delivered daily.

DARPA posts quantum computing RFI

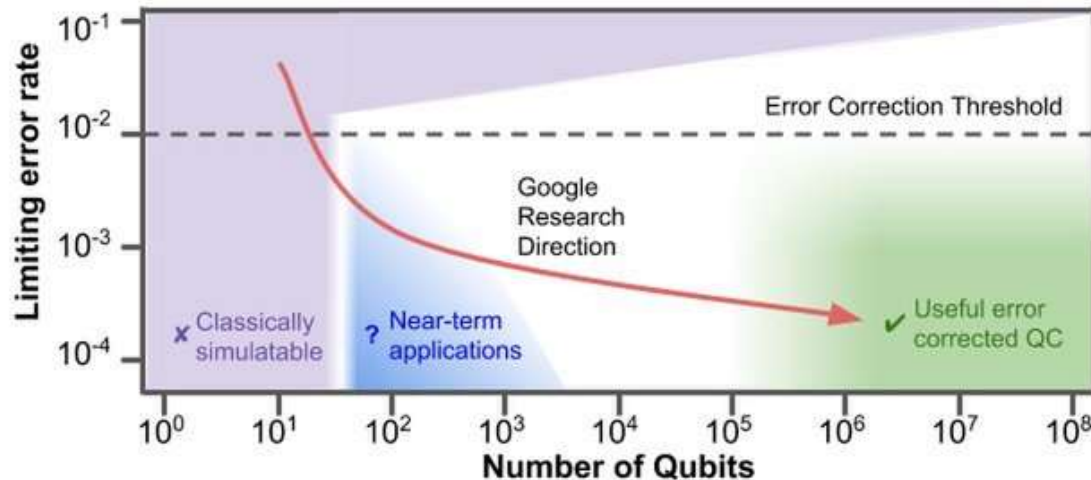
DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA) REQUEST FOR INFORMATION

DARPA

On July 20, the Defense Advanced Research Projects Agency (DARPA) posted a request for information for Quantum Computing Applications with State-of-the-Art Capabilities (Solicitation Number: DARPA-SK-18-001). Responses are due by 4:00 p.m. Eastern on August 20.

* The Defense Advanced Research Projects Agency (DARPA) Defense Science and Office (DSO) is seeking information on new capabilities that could be enabled by quantum computing.

Universal Gate Quantum Computing

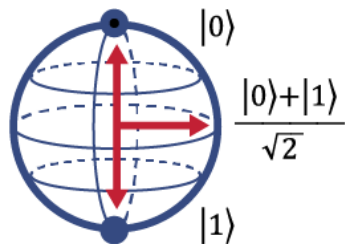


Is Quantum Computing the next major Paradigm?

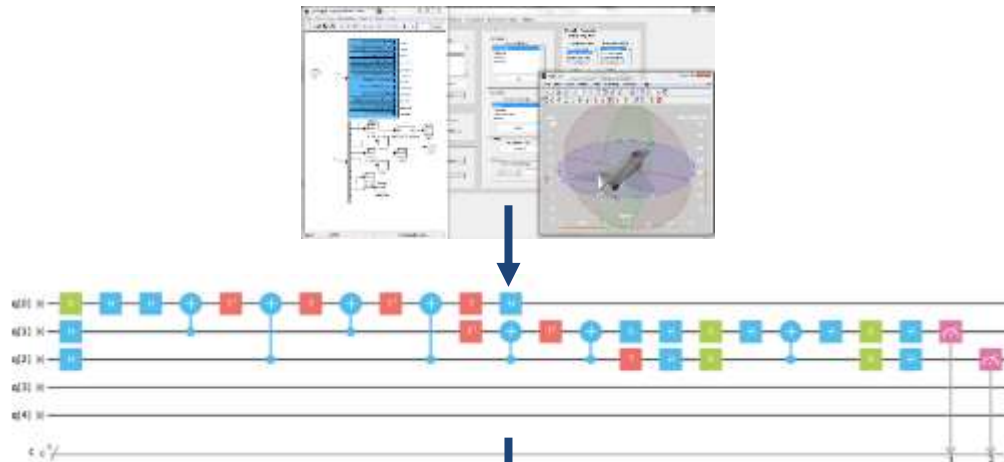
What is the path to mission-capable...

Quantum Software Engineering

● 0
● 1
Classical Bit



Qubit



What are we doing?

So

Sat

- S
- (
- S
- (

Combinatorial?

$X = 1$

<http://satcompetition.org/>

Why is it significant?

Quantum Speedup and Software VV

Grover's Algorithm (SAT):

$$(V_1 \vee V_2 \vee V_3) \wedge \neg(\neg V_1 \vee \neg V_2 \vee V_3) \wedge \dots$$

Grover's algorithm: quantum search algorithm that finds with high probability the unique input to a black box function that produces a particular output value, using just **$O(\sqrt{N})$** evaluations of the function, where **N** is the size of the function's domain.

```
int get_sign(int x) {  
    if (x == 0)  
        return 0;  
  
    if (x < 0)  
        return -1;  
    else  
        return 1;  
}
```

SMT

$X = 0$

$X = -1$

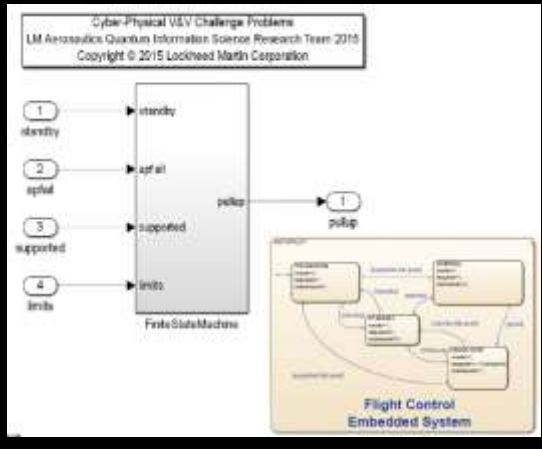
$X = 1$

classical $O(2^n)$ -> quantum $O(2^{n/2})$

<http://satcompetition.org/>

What are we going to do?

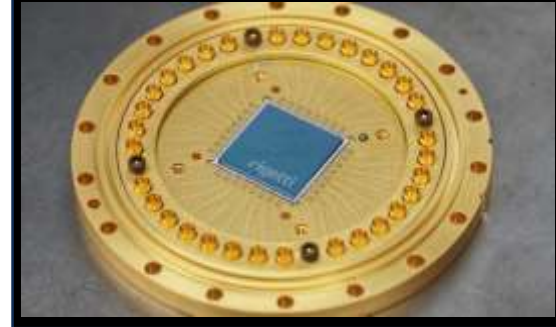
Lockheed Martin Challenge Problem



Satisfiability (SAT) Solver

```
int get_sign(int x) {  
    if (x == 0)  
        return 0;  
  
    if (x < 0)  
        return -1;  
    else  
        return 1;  
}
```

Quantum Universal Gate



Benchmarking

SAT Solver (Grover's Algorithm):

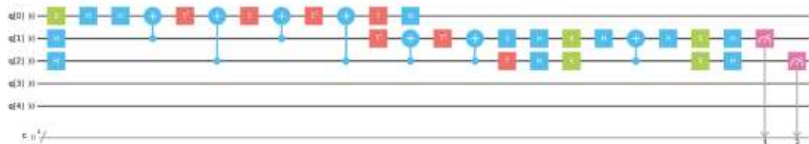
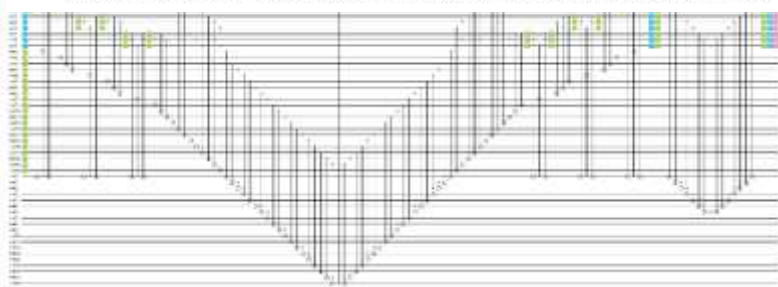


FIG. 2: The circuit that was executed on IBM's 5-qubit quantum computer (ibmqv4 was used). The first two time slots correspond to the state preparation. The next 13 time slots implement a Toffoli gate. The next 7 time slots implement the $2|\psi\rangle\langle\psi| - I$ operator, and the final two time slots are used for observing x_1 and x_2 .



$(v_1 \vee v_2) \wedge (v_1 \vee v_3) \wedge (v_2 \vee v_3)$ (50 qubits)

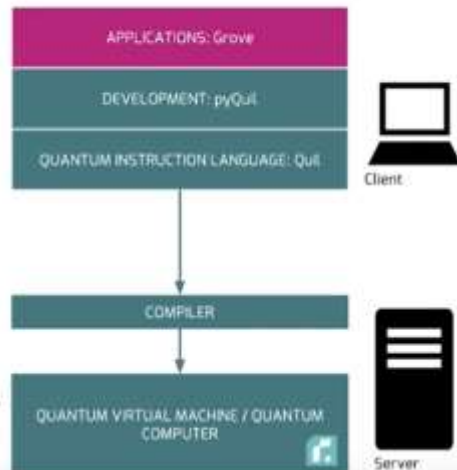
LM Challenge Problem... (? qubits)

Automatically Solving NP-Complete Problems on a Quantum Computer
ICSE '18 Companion, May 27-June 3, 2018, Gothenburg, Sweden

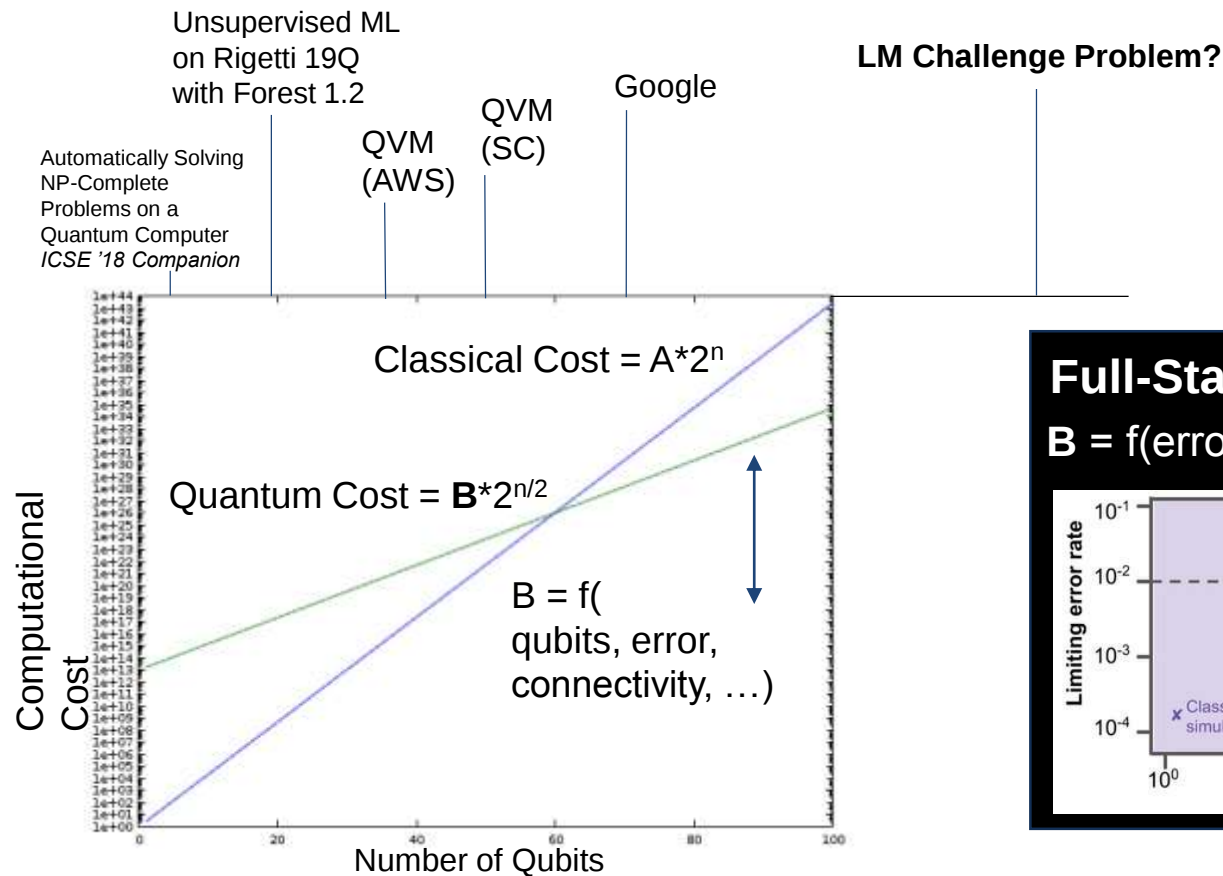
Full-Stack Software Universal Gate

FOREST

- > Write applications...
- > using tools...
- > that build quantum programs...
- > that compile onto quantum hardware...
- > that execute on a real or virtual quantum processor.

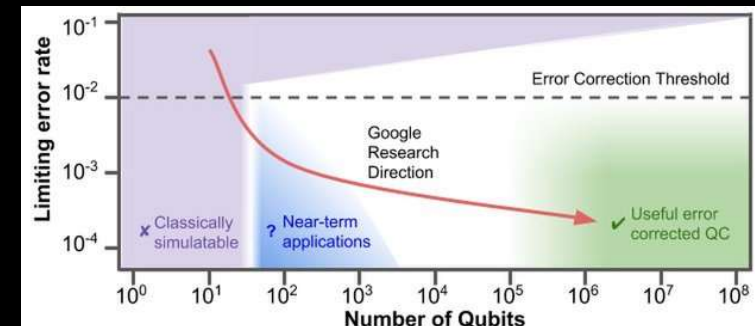


Deliverable: Projection for LM Challenge Problem



Full-Stack Engineering

$$B = f(\text{error, connectivity, ...})$$



Questions?



Dr. Jason Larkin
Research Scientist Quantum
Physics, HPC, Software VV

Quantum Physics and Computing

PhD Thesis “Thermal Transport Properties of Disordered Materials from High Performance Atomistic Simulations”

Quantum Chemistry (DFT), Quantum Computing for Quantum Chemistry
HPC
AFRL, DoD HPCMP

Software VV

SpiralGen: DARPA High-Assurance Cyber Military Systems (HACMS)

[“High-Assurance SPIRAL: End-to-End Guarantees for Robot and Car Control”](#), IEEE Control Systems Magazine, 2017.

[“High Assurance Spiral: Scalable and Performance Portable Domain-Specific Control System Synthesis”](#).

SEI: GraphBLAS

A Test Framework for GraphBLAS (ICSE 2019, in progress)