

# ORNL's AI Initiative: Advancing Secure, Trustworthy, and Energy-Efficient AI for Science

Prasanna Balaprakash

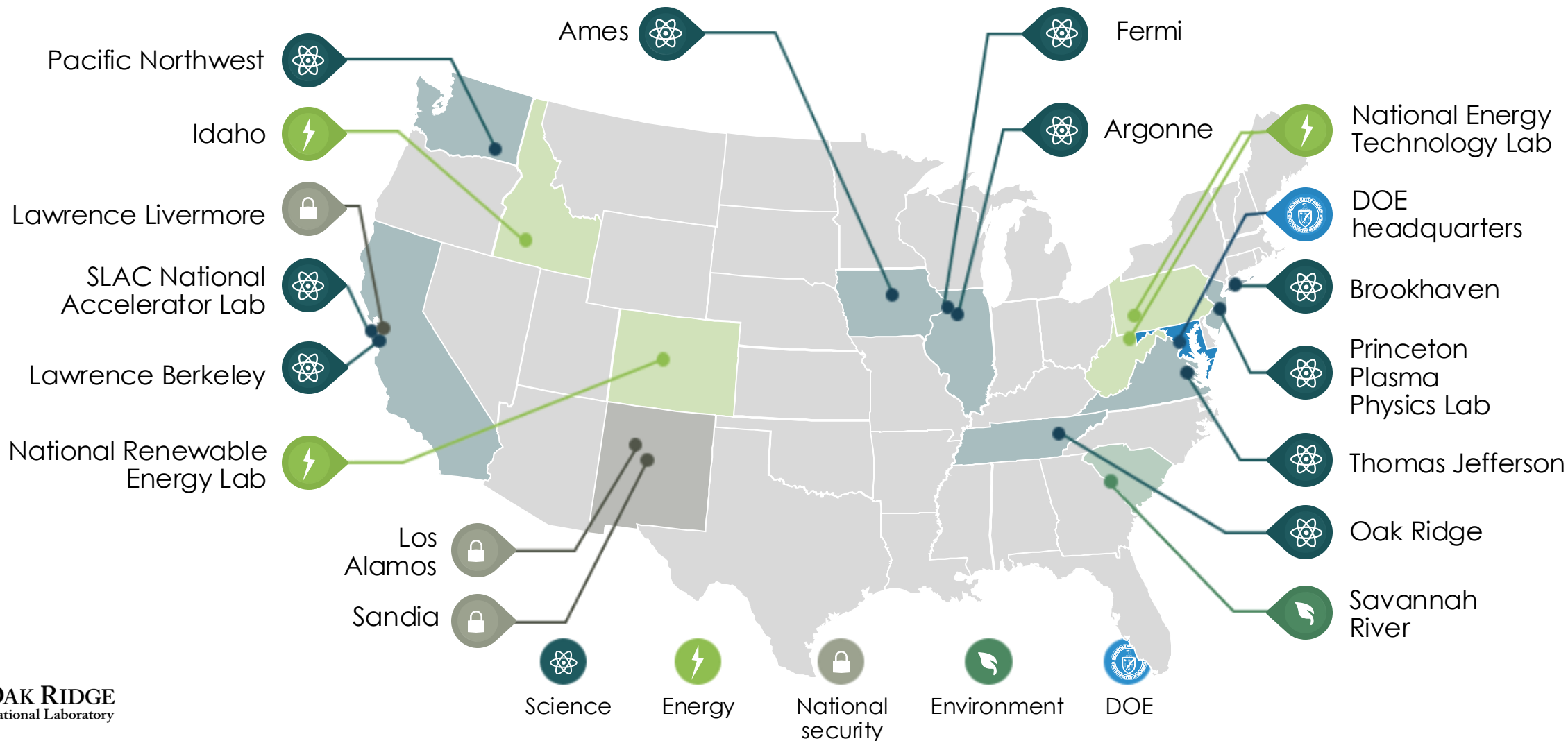
Director of AI Programs

Oak Ridge National Laboratory



ORNL is managed by UT-Battelle LLC for the US Department of Energy

# Department of Energy National Labs: Born from the Manhattan Project, now lead research in energy, security, and advanced technologies.



# ORNL's mission

---

Deliver scientific discoveries and technical breakthroughs needed to realize solutions in clean energy and national security and provide economic benefit to the nation





# ORNL has a rich history leveraging AI for science



**1979**  
Oak Ridge  
Applied Artificial  
Intelligence  
Project



**1991**  
Automated  
machines



**Current  
Frontier**

- #1 HPL-MxP @10 exaflops for AI
- #2 on GREEN500
- 2021 ACM A.M. Turing Award
- Scaled to 1T+ parameter AI model training

1940–1970

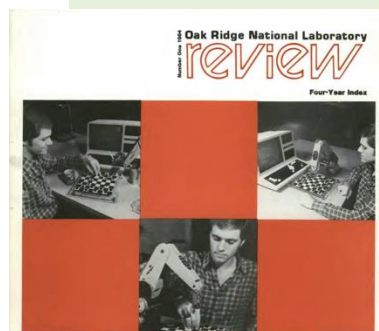
1980

1990

2000



**1981**  
AI infrastructure  
supports  
spectroscopy,  
environmental  
management,  
nuclear fuel  
reprocessing,  
and programming  
assistance



**1983**  
Robotics



**2017**  
Summit:  
World's "smartest"  
supercomputer  
optimized for AI

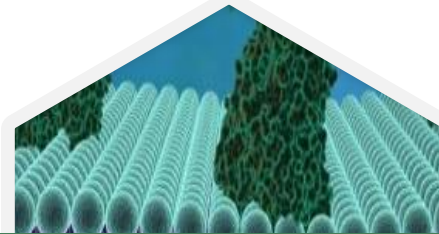
# AI is transforming science at ORNL



**Spallation  
Neutron Source**



**Manufacturing  
Demonstration Facility**



**Center for Structural  
Molecular Biology**



**Oak Ridge Leadership  
Computing Facility**



**Cyber Science  
Research Facility**



**High Flux  
Isotope Reactor**

# Grand challenges in AI

The promise of AI is challenged by lack of:

- Safety
- Security
- Trustworthiness
- Energy efficiency

Smithsonian  
MAGAZINE

SUBSCRIBE

SMART NEWS

## 'Hallucinate' Is Dictionary.com's Word of the Year for 2023

In the context of artificial intelligence, the word means "to produce false information" and "present it as if true"

 Sarah Kuta  
Daily Correspondent  
December 15, 2023

nature

Explore content ▾ About the journal ▾ Publish with us ▾ | Subscribe

[nature](#) > [news](#) > article

NEWS | 01 October 2024

## 'In awe': scientists impressed by latest ChatGPT model o1


The chatbot excels at science, beating PhD scholars on a hard science test. But it might 'hallucinate' more than its predecessors.

SEARCH FORTUNE SIGN IN [Subscribe Now](#)

Home News Tech Finance Leadership Well Recommendations Fortune 500

TECH · BRAINSTORM AI

## AI could gobble up a quarter of all electricity in the U.S. by 2030 if it doesn't break its energy addiction, says Arm Holdings exec



# AI executive order is focused on grand challenges

OCTOBER 30, 2023

## Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence



▶ BRIEFING ROOM ▶ PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:



# Paradox of AI development

Easy to demo but hard in production

Hard problems are easy and the easy problems are hard

Ever growing open research problems

Humans remain a roadblock

Unique challenges with cyber-physical systems





# Misalignment



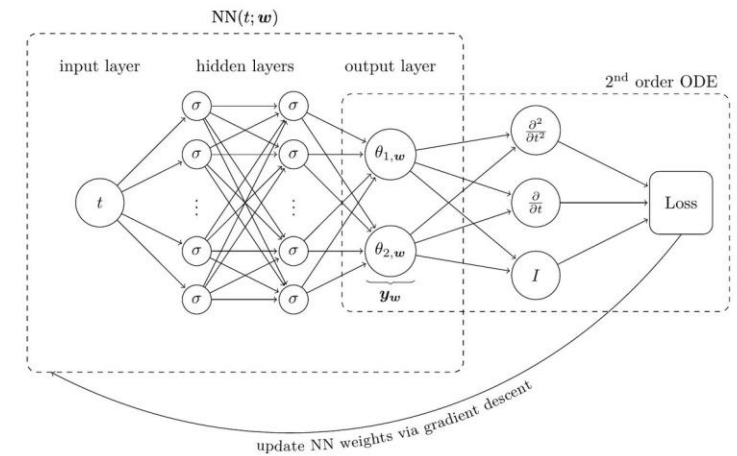
<https://openai.com/research/faulty-reward-functions>

## How PINNs cheat: Predicting chaotic motion of a double pendulum

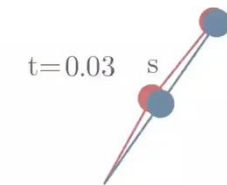
**Sophie Steger**  
Graz University of Technology  
Graz, Austria  
sophie.steger@tugraz.at

**Franz M. Rohrhofer**  
Know-Center GmbH  
Graz, Austria  
frohrhofer@know-center.at

**Bernhard C. Geiger**  
Know-Center GmbH  
Graz, Austria  
bgeiger@know-center.at



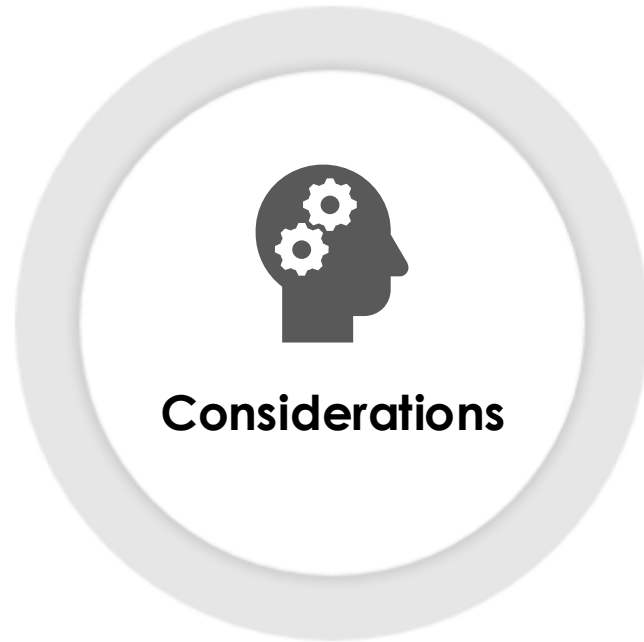
PINN



Runge-Kutta

# Multifaceted AI development

Develop methods to establish trust in AI systems, focusing on uncertainty, validation, causality, and privacy



Accuracy

Fairness

Privacy

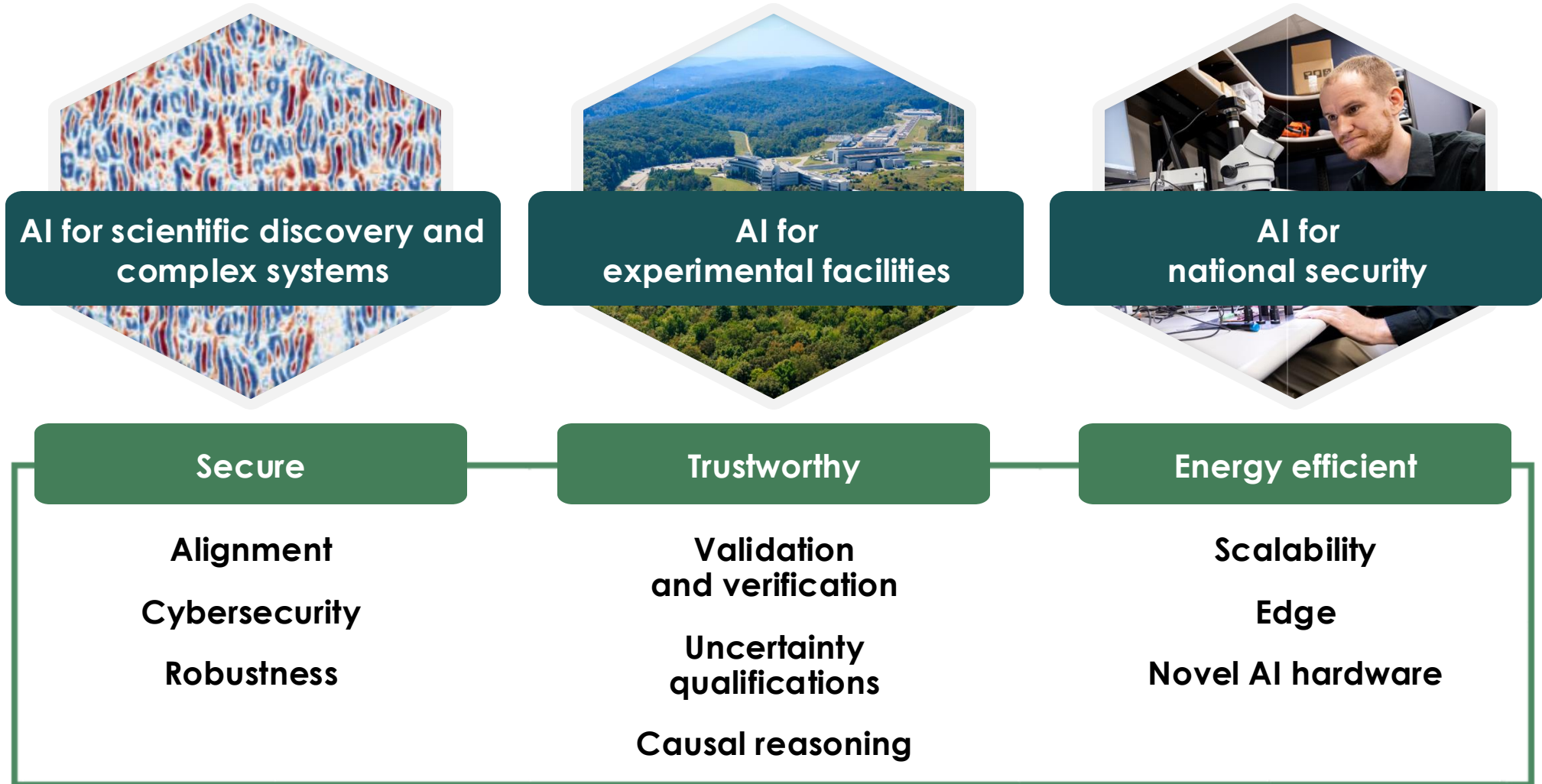
Transparency

Robustness

Energy-  
efficiency

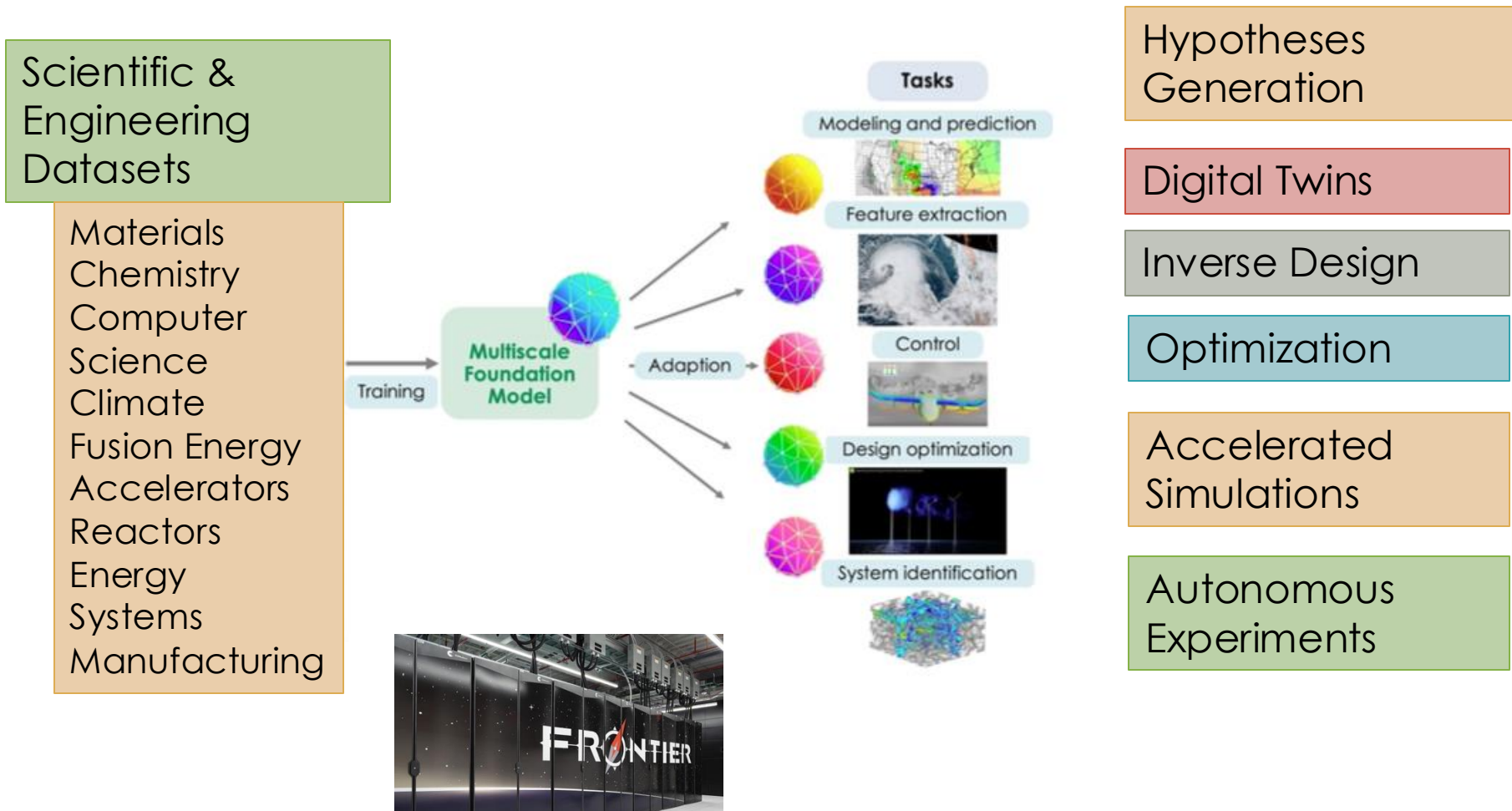
# ORNL's AI initiative

Secure, trustworthy, and energy-efficient AI





# Foundation AI model(s) for science



# First open-source instantiation of a trillion-parameter model on Frontier

Since the model is too large to fit in one GPU's memory, we **automated the distribution of model across multiple GPUs** using multi-dimensional parallelization

- First time setting and on non-NVIDIA hardware in open science
- Achieved more than 80% efficiency (best use of hardware and thus energy efficient)
- Democratized recipe for the benefit of the scientific community



Sajal Dash and team

Frontier trained a ChatGPT-sized large language model with only 3,000 of its 37,888 Radeon GPUs — the world's fastest supercomputer blasts through one trillion parameter model with only 8 percent of its MI250X GPUs

News

By Matthew Connatser published January 07, 2024

Now you're playing with AI power!

      Comments (19)

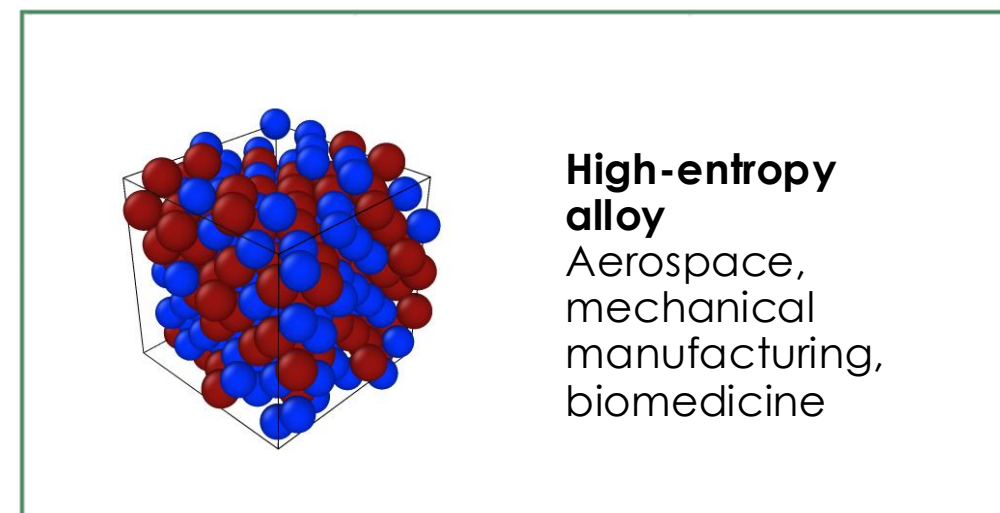
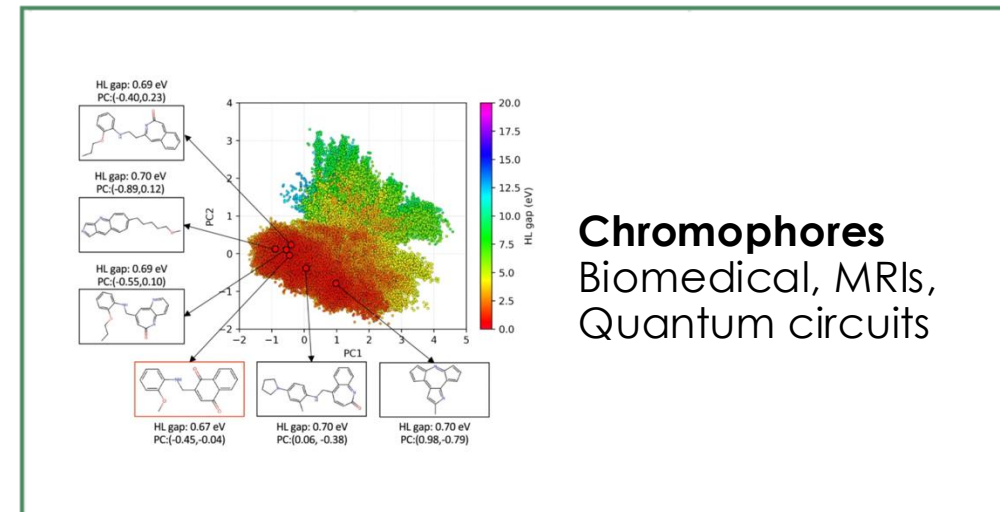
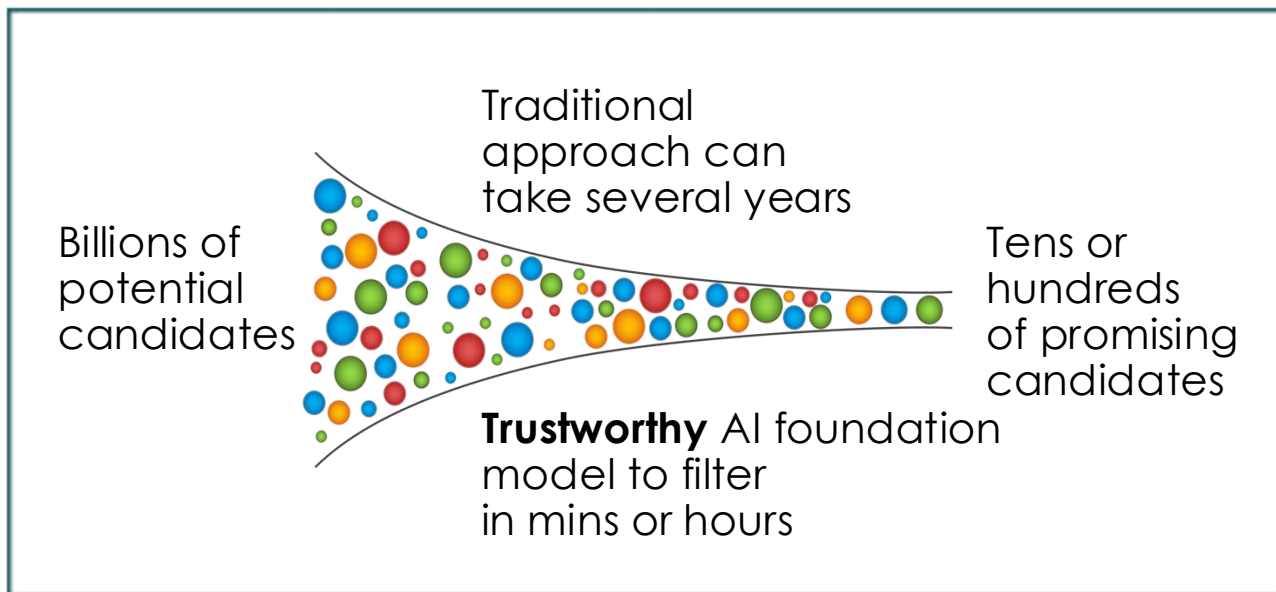


 OAK RIDGE National Laboratory

(Image credit: ORNL)

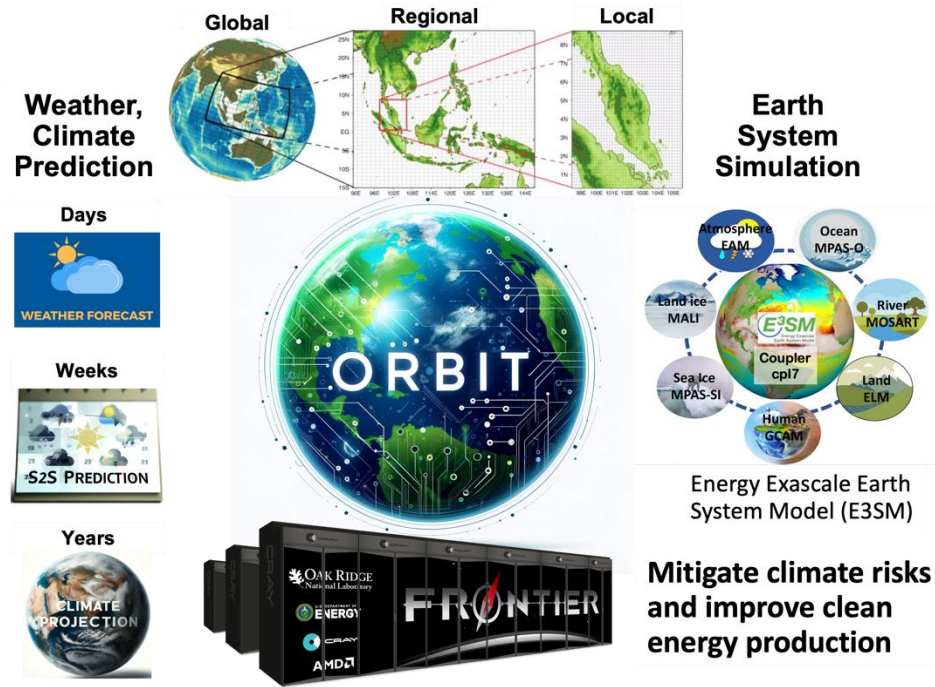
Researchers at Oak Ridge National Laboratory trained a large language model (LLM) the size of ChatGPT on the Frontier supercomputer and only needed 3,072 of its 37,888 GPUs to do it. [The team published a research paper](#) that details

# Accelerated materials discovery via trustworthy AI models on Frontier

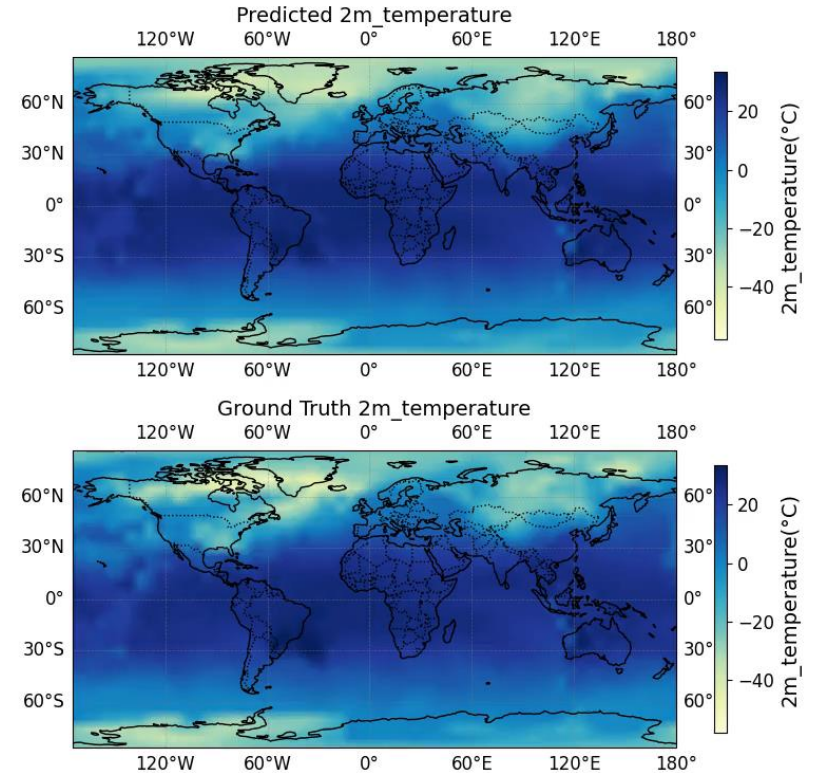




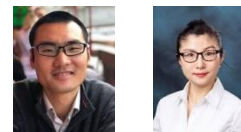
# Trustworthy AI model for accurate weather and climate predictions



Variable 2m\_temperature, at time: 2017-01-04 02:00, lead time: 72 hrs



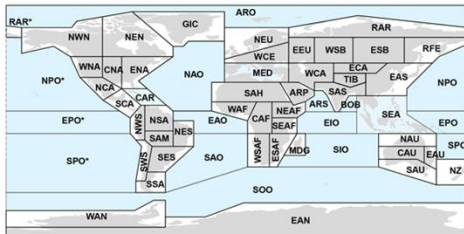
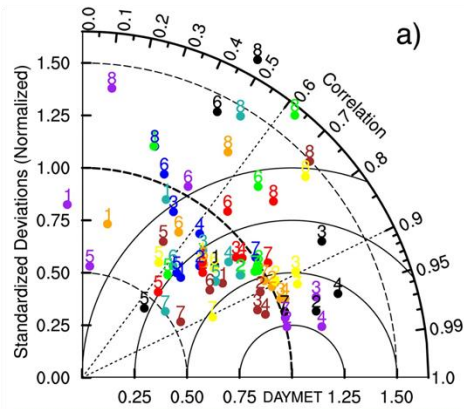
- Developed a large-scale AI foundation model (FM), pretrained on CMIP6 model simulation data and adaptable to various Earth system modeling tasks.
- Using 49,152 GPUs on 6,144 Frontier nodes, ORBIT achieves 70% scaling efficiency with a computing throughput of 1.6 exaflops ([finalist for the 2024 Gordon Bell Prize for Climate Modelling](#)).
- ORBIT achieves competitive or better accuracy in forecasting critical atmospheric variables up to 30 days ahead.



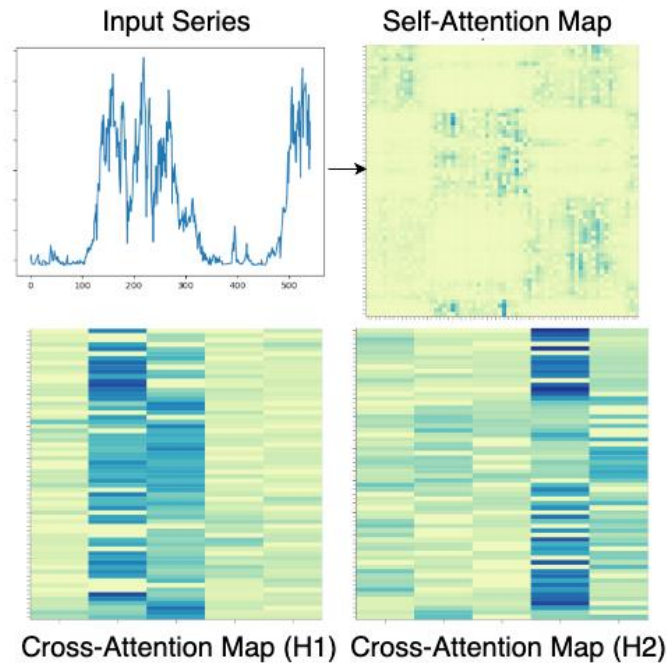
# Trustworthy AI

Develop foundational methods to establish trust in AI systems, focusing on uncertainty, validation, causality, and privacy

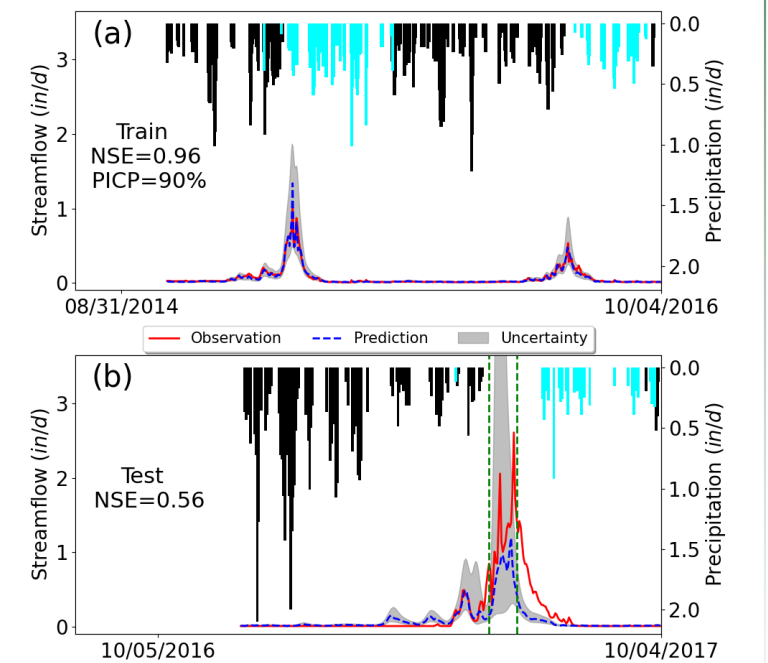
## V&V to ensure accuracy and reliability



## Analysis to ensure physical consistency

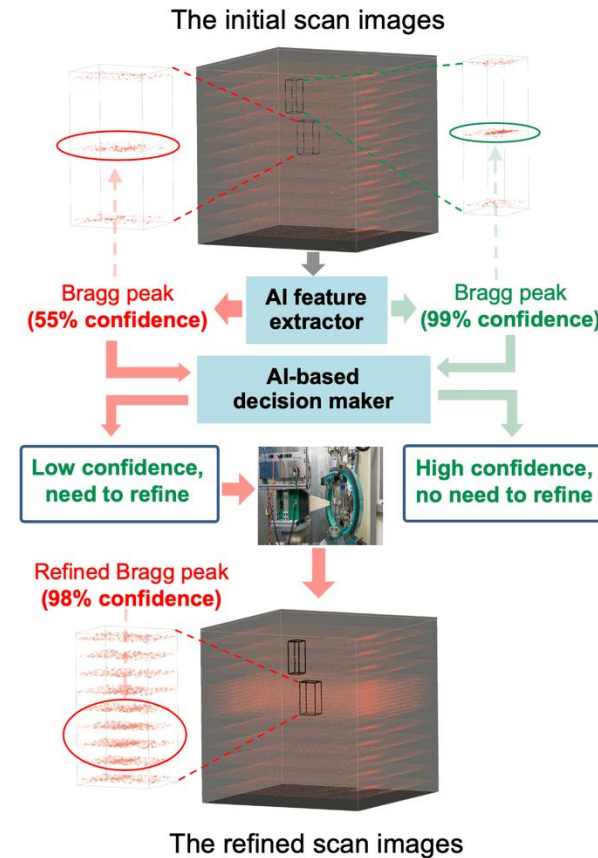
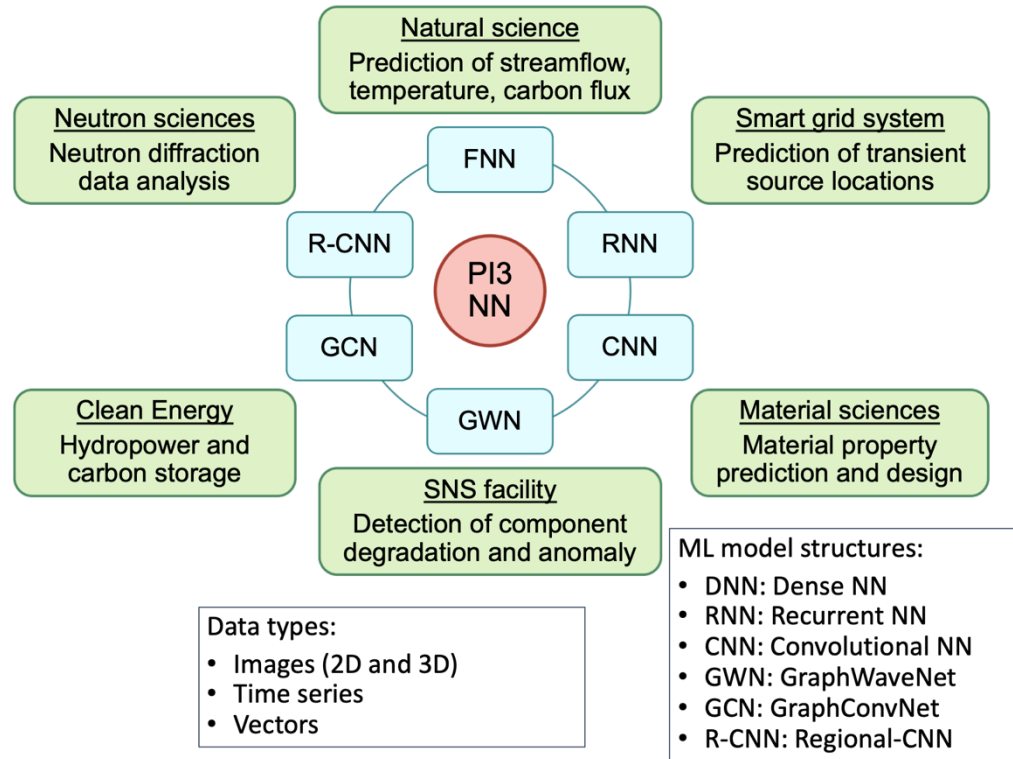


## Uncertainty analysis to ensure reliable prediction



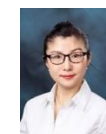
# Efficient uncertainty quantification for trustworthy AI

Develop UQ methods for trustworthy AI model predictions which supports risk-aware decision making and advances scientific discovery.



- Our UQ method enabled neutron diffraction experiment automation;
- It optimizes beam usage ~50% efficiency.
- The optimized usage of beamline increase science productivity by ~2X.

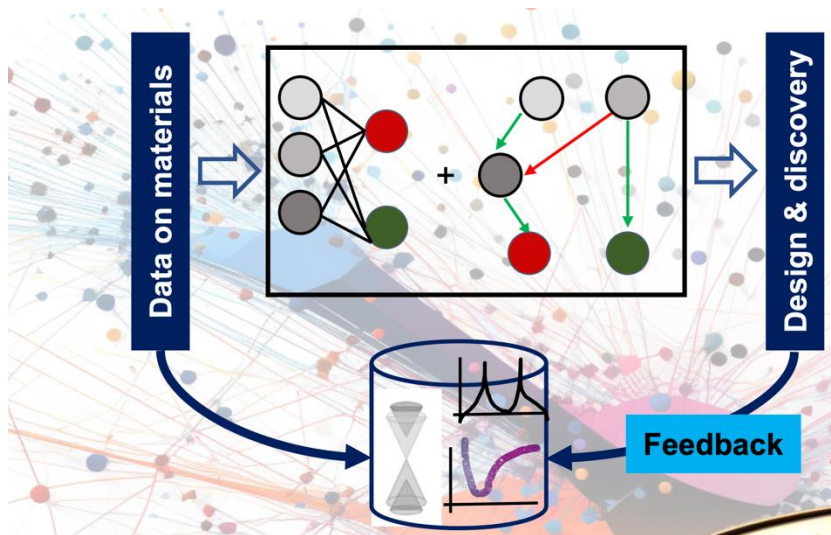
Our UQ method has been successfully applied across multiple DOE-mission applications to advance the scientific discovery and facilitate clean energy generation.



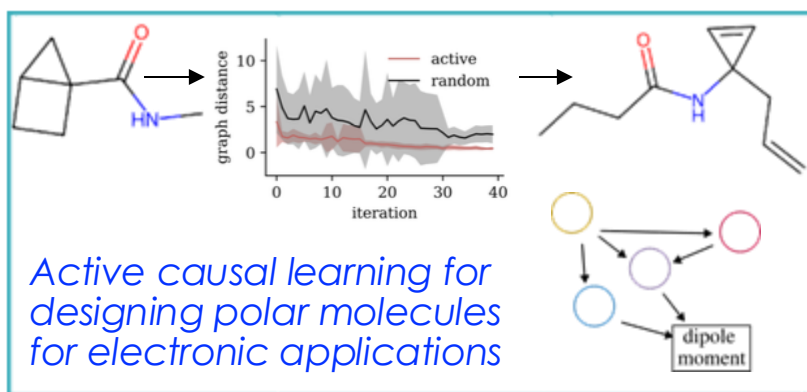


# Causal AI for trustworthy scientific solutions

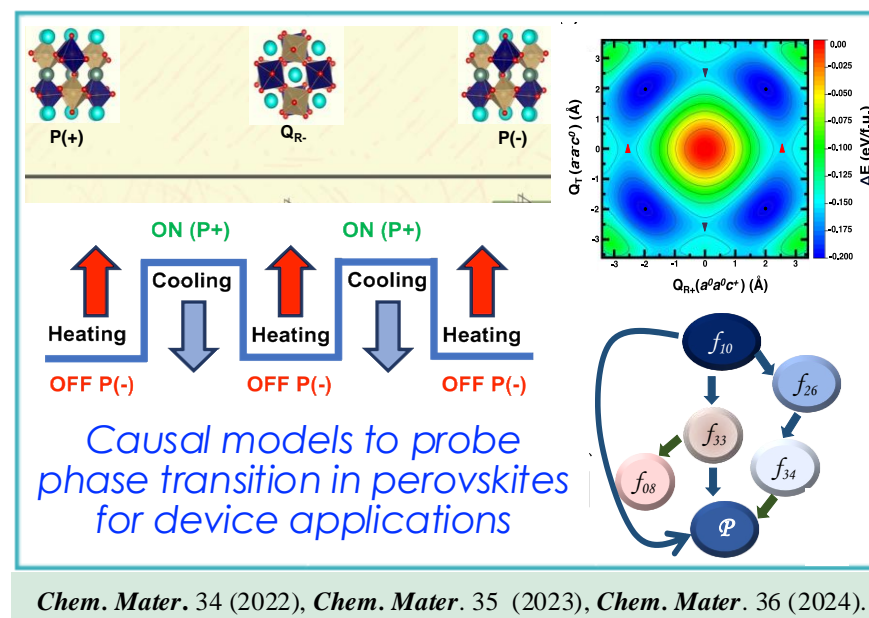
Develop causal AI models for discovering materials and process optimization with targeted applications in chemistry, biology and materials sciences



Generalized Causal AI workflow to guide reliable & trustworthy materials design & discovery

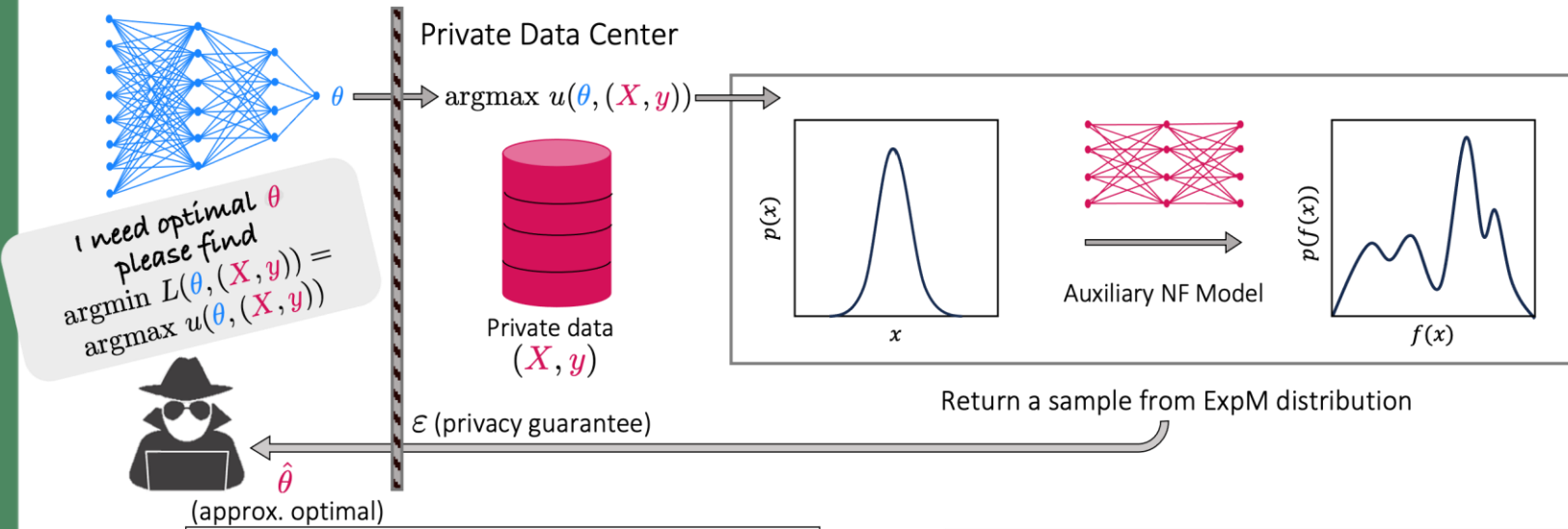


*AI4Mat NeurIPS workshop* (2023), *Comp. Mater. Sci.* 233 (2024).



Ayana Ghosh and team

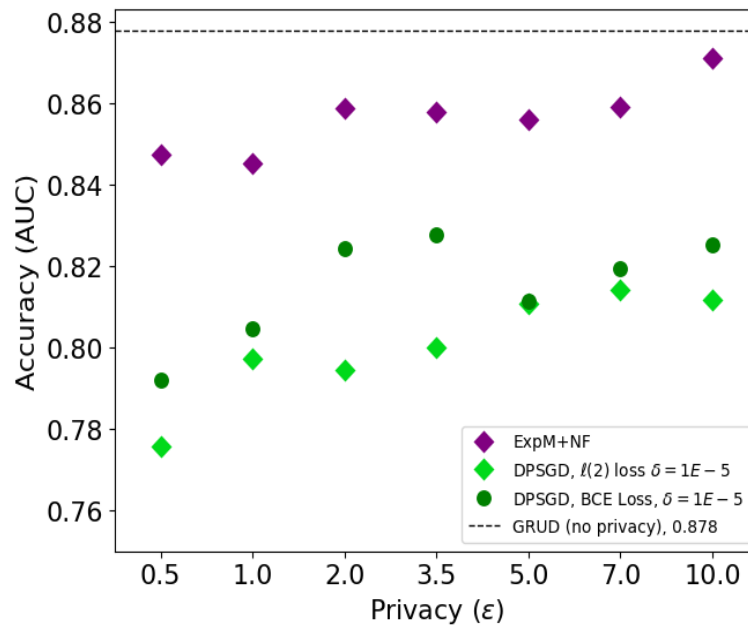
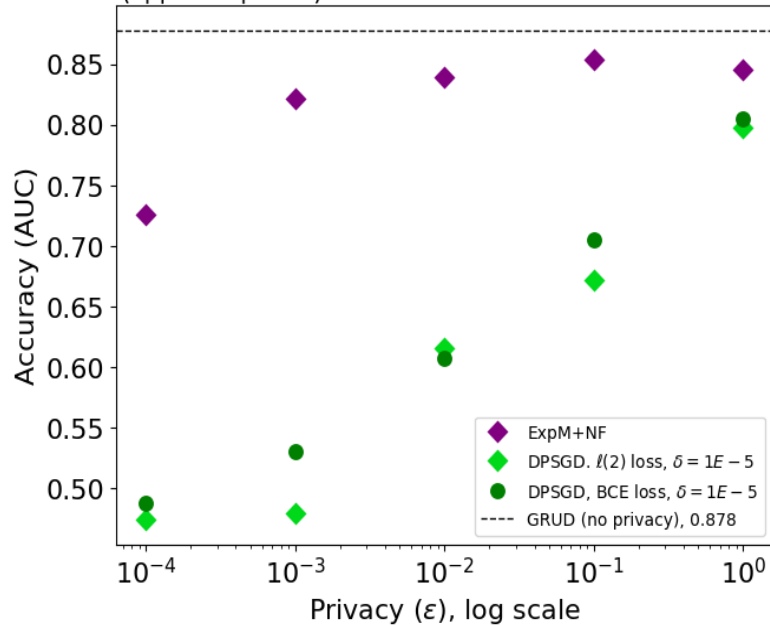
# Transformational approach to differentially private ML



**Setting:** Need to train and release ML on a private dataset with a formal privacy guarantee

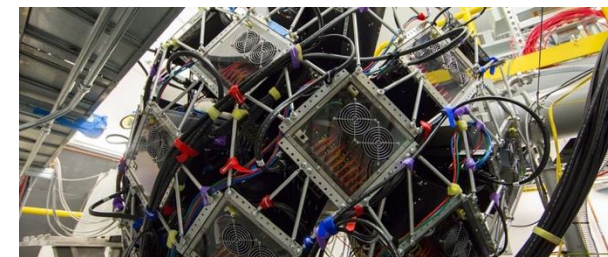
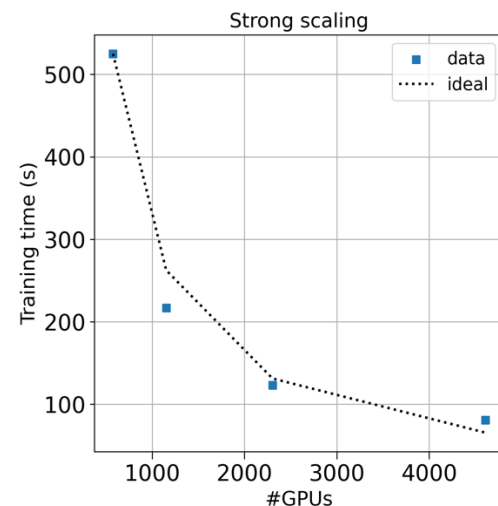
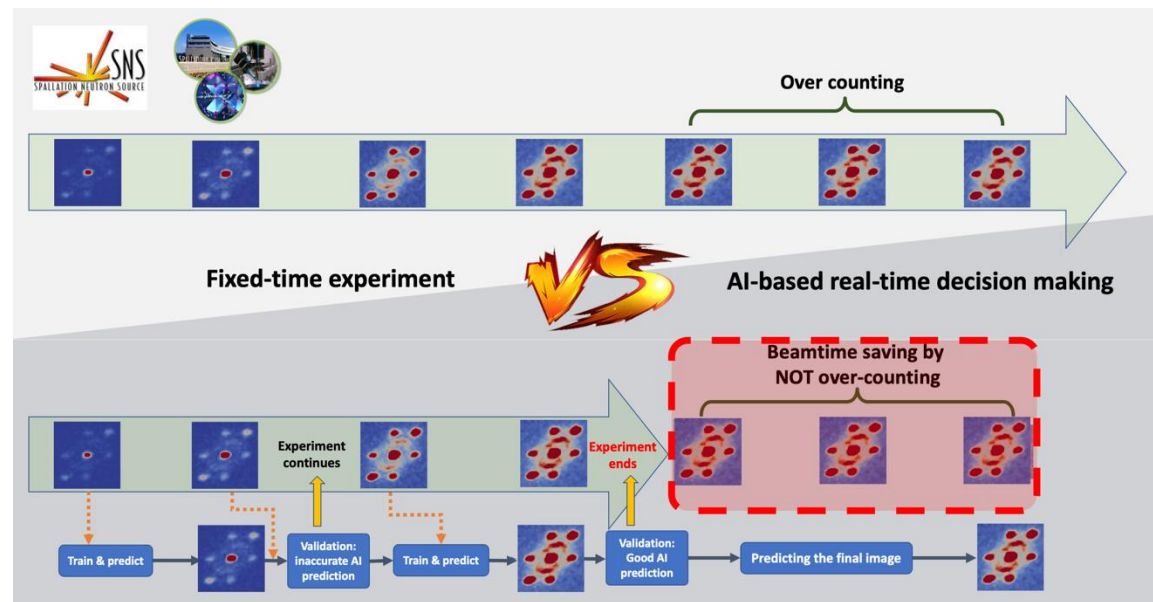
**Approach:** Leverage Exponential Mechanism (ExpM), which has a historically intractable distribution + an auxiliary normalizing flow (NF) model to approximately sampling from the required density

**Results:** Can a model be trained by ExpM+NF? Yes! ExpM+NF-trained models have similar accuracy with three orders of magnitude smaller (better) privacy parameter than DPGSD (SOTA).



# Frontier-enabled AI for real-time experiment steering at neutron facilities

- Time-of-flight neutron instruments (e.g., TOPAZ) produce large data that require AI+HPC to enable real-time data analysis and decision making.
- Our AI model on Frontier can process live neutron data from TOPAZ, analyze it in real-time, and decide when to end the experiment to save neutron beamtime.
- AI model could reduce the experiment time by around 30% at TOPAZ.
- AI system can increase the number of experiments that can be done within each experiment cycle at SNS and the future STS.



We demonstrated our AI method on TOPAZ data generated at SNS

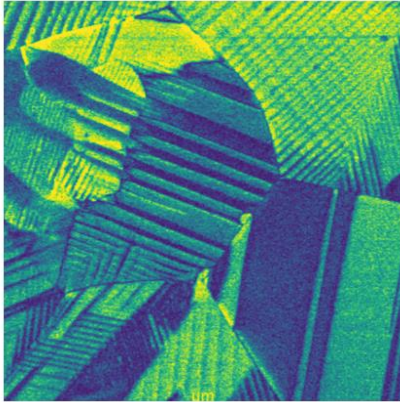
**Outstanding scalability on Frontier with up to 4608 GPUs.**



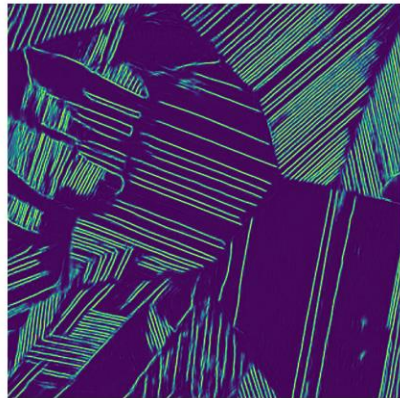


# Tiny AI and edge computing for materials characterization

## Imaging



## Inference



Instrument

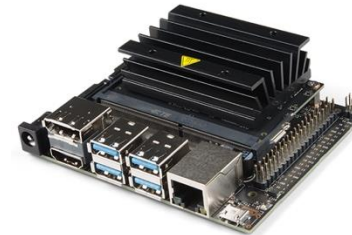
~64 MB/s

~ MB-GB/run

## "Streaming" Edge



FPGA\*



Jetson Nano

## GPU "Far" Edge



Model Training  
DGX-2 16 GPUs

## Feedback for control

- Real time segmentation for autonomous characterization
- Model training and refinement to handle out of distribution effects



Narasinga Rao  
Miniskar and team

# AI security research: Understanding risks and threats

A new field of research at the intersection of AI and cyber security research



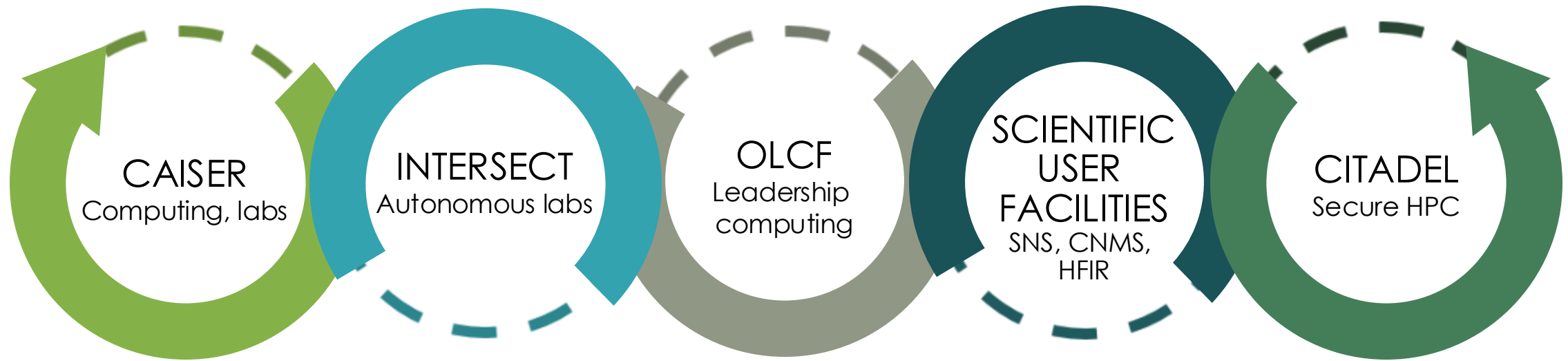
**2 critical facets of AI security research:**  
What are the threats emanating from AI systems?  
What are the threats to AI systems?

# Center for AI Security Research (CAISER)

**CAISER** utilize ORNL's world class resources to analyze vulnerabilities, threats, and risks related to the security and misuse of AI.



# The ORNL AI LDRD initiative leverages other ORNL initiatives and facilities to magnify impact





# ORNL's AI Academy

- AI Summer Institute
- AI Tutorial Series for Science
- AI for Science Bootcamps
- AI Workshops
- AI Expo
- AI Seminar Series





# FASST: Frontiers in Artificial Intelligence for Science, Security, and Technology

Federation News & Analysis Students Careers Diversity Library About

## FYI: Science Policy News


FYI HOME ARTICLES BUDGET TRACKER BILL TRACKER AGENCIES ABOUT FYI

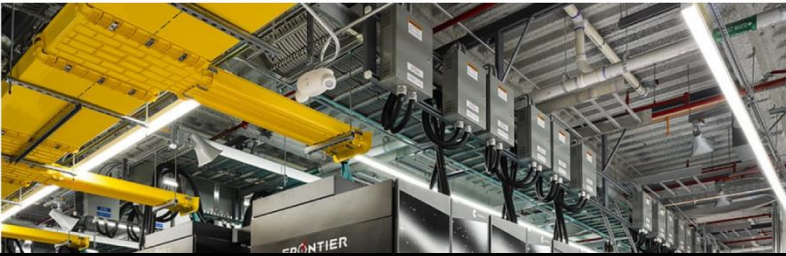
FYI / ARTICLE

### DOE Labs Pitching Major AI R&D Initiative to Congress

AUG 11, 2023

Department of Energy national labs are laying groundwork for a potential multi-billion dollar initiative to develop artificial intelligence tools for scientific and security applications, leveraging its advanced computing capabilities.

 Jacob Taylor



ANL-22/91

## ADVANCED RESEARCH DIRECTIONS ON AI FOR SCIENCE, ENERGY, AND SECURITY

### Report on Summer 2022 Workshops

**Jonathan Carter**  
*Lawrence Berkeley National Laboratory*

**John Feddema**  
*Sandia National Laboratories*

**Doug Kothe**  
*Oak Ridge National Laboratory*

**Rob Neely**  
*Lawrence Livermore National Laboratory*

**Jason Pruet**  
*Los Alamos National Laboratory*

**Rick Stevens**  
*Argonne National Laboratory*

U.S. DEPARTMENT OF ENERGY U.S. DEPARTMENT OF ENERGY Office of Science NIS National Nuclear Security Administration

ANL-23/89

## ADVANCED RESEARCH DIRECTIONS ON AI FOR ENERGY

### Report on Winter 2023 Workshops

**Claus Daniel**  
*Argonne National Laboratory*

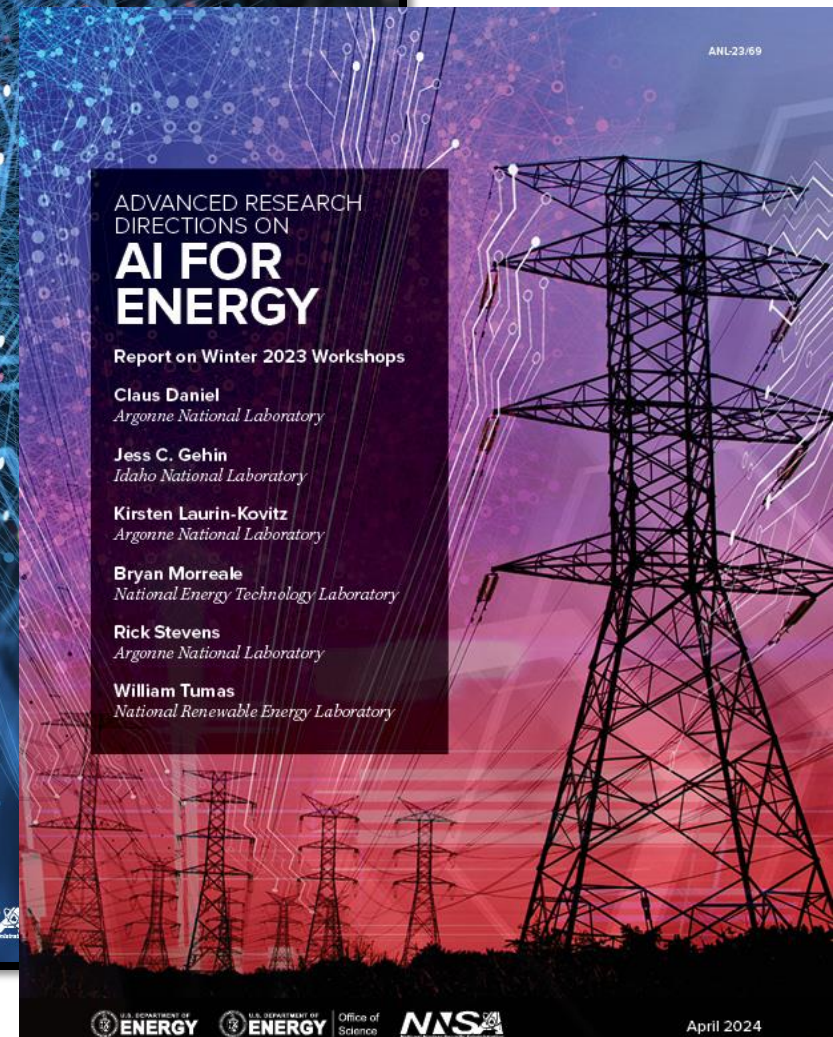
**Jess C. Gehin**  
*Idaho National Laboratory*

**Kirsten Laurin-Kovitz**  
*Argonne National Laboratory*

**Bryan Morreale**  
*National Energy Technology Laboratory*

**Rick Stevens**  
*Argonne National Laboratory*

**William Tumas**  
*National Renewable Energy Laboratory*



U.S. DEPARTMENT OF ENERGY U.S. DEPARTMENT OF ENERGY Office of Science NIS National Nuclear Security Administration



# FASST: Frontiers in Artificial Intelligence for Science, Security, and Technology

*FASST will build the world's most powerful integrated scientific AI systems through four key interconnected pillars:*

## **Pillar 1**

**AI-Ready Data.** Data is the fuel that drives the engine of AI. FASST will transform DOE's vast repositories of classified and unclassified scientific data into the world's largest, high-quality repository of AI-ready

## **Pillar 2**

**Frontier-Scale AI Computing Infrastructure and Platforms.** FASST will build the next generation of energy efficient AI-enabled supercomputing platforms and algorithms capable of seamlessly merging

## **Pillar 3**

**Safe, Secure, and Trustworthy AI Models and Systems.** Combining DOE's scientific and engineering data with commensurate computing power, DOE will build, train, test, and validate frontier-class AI

## **Pillar 4**

**AI Applications.** AI models developed through FASST will revolutionize the way DOE delivers on its science, energy, and security mission. AI-accelerated scientific discoveries can lead to affordable batteries

# FASST is focused on six crosscutting themes

## AI for advanced properties inference and inverse design

Energy Storage  
Proteins, Polymers,  
Stockpile modernization

## AI and robotics for autonomous discovery

Materials, Chemistry, Biology  
Light-Sources, Neutrons

## AI-based surrogates for high-performance computing

Climate Ensembles  
Exascale apps with surrogates  
1000x faster => Zettascale now

## AI for software engineering and programming

Code Translation, Optimization  
Quantum Compilation, QAlgs

## AI for prediction and control of complex engineered systems

Accelerators, Buildings, Cities  
Reactors, Power Grid, Networks

## Foundation, Assured AI for scientific knowledge

Hypothesis Formation, Math  
Theory and Modeling Synthesis,



# FASST: Frontiers in Artificial Intelligence for Science, Security, and Technology

🏠 Sections ▾ 👁 Browse ▾ 🔍 Search ▾ ⚙ Reader Aids ▾ 👤 My FR ▾  🔍



## FEDERAL REGISTER

The Daily Journal of the United States Government



**N** Notice

**Design Updates:** As part of our ongoing effort to make FederalRegister.gov more accessible and easier to use we've enlarged the space available to the document content and moved all document related data into the utility bar on the left of the document. [Read more in our feature announcement.](#)

## Notice of Request for Information (RFI) on Frontiers in AI for Science, Security, and Technology (FASST) Initiative

A Notice by the [Energy Department](#) on 09/12/2024



<https://www.federalregister.gov/documents/2024/09/12/2024-20676/notice-of-request-for-information-rfi-on-frontiers-in-ai-for-science-security-and-technology-fasst>

# Michael Levitt: Studied Physics, Masters Biology, Won Nobel in Chemistry

HOME TRAINING NUTRITION HEALTH MIND TECH BUSINESS GEAR ABOUT CONTACT



TECH GREAT MINDS

## Nobel laureate Dr Michael Levitt: AI will change everything forever

The decorated and respected scientist, an early adopter of ChatGPT and other AI technologies, reveals whether the rapid emergence of ever-more powerful machine learning tools will ultimately help or harm humanity as it changes our world beyond recognition



BY JOE WARNER SEPTEMBER 11, 2024



# Nobel prizes for AI



**NOBELPRISET I KEMI 2024**  
**THE NOBEL PRIZE IN CHEMISTRY 2024**

KUNGL. VETENSKAPS-  
AKADEMIEN  
THE ROYAL SWEDISH ACADEMY OF SCIENCES

**David Baker**  
University of Washington  
USA

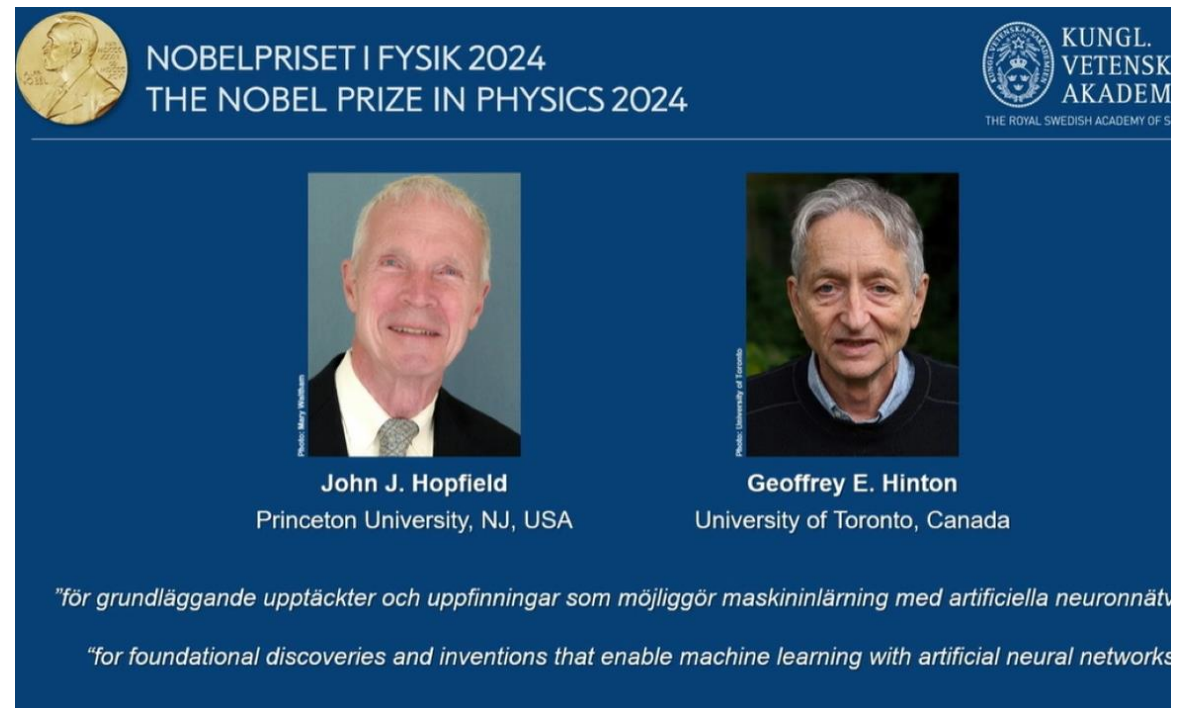
**Demis Hassabis**  
Google DeepMind  
United Kingdom

**John M. Jumper**  
Google DeepMind  
United Kingdom

*"för datorbaserad proteindesign"*  
*"for computational protein design"*

*"för proteinstrukturprediktion"*  
*"for protein structure prediction"*

THE NOBEL PRIZE



**NOBELPRISET I FYSIK 2024**  
**THE NOBEL PRIZE IN PHYSICS 2024**

KUNGL. VETENSKAPS-  
AKADEMIEN  
THE ROYAL SWEDISH ACADEMY OF SCIENCES

**John J. Hopfield**  
Princeton University, NJ, USA

**Geoffrey E. Hinton**  
University of Toronto, Canada

*"för grundläggande upptäckter och uppfinningar som möjliggör maskininläring med artificiella neuronnät"*  
*"for foundational discoveries and inventions that enable machine learning with artificial neural networks"*