**Pressfile**

Total of characters: 29242

1. Using artificial intelligence to engineer materials’ properties. February the 11th 2019, <http://news.mit.edu/2019/artificial-intelligence-engineer-microchips-0211> , 7605 (Page 2 à 5)
2. A faster, more efficient cryptocurrency, January the 23th 2019, <http://news.mit.edu/2019/vault-faster-more-efficient-cryptocurrency-0124> , 7829 (Page 6 à 8)
3. Fortifying the future of cyptography, January the 16th 2019, <http://news.mit.edu/2019/faculty-vinod-vaikuntanathan-0116> , 7557 (Page 9 à 11)
4. Using machine learning for medical solutions, March the 19th 2019, <http://news.mit.edu/2019/student-kyle-swanson-computer-science-0319> , 6251 (Page 12 à 13)

news.mit.edu, 02/11/2019

<http://news.mit.edu/2019/artificial-intelligence-engineer-microchips-0211>

# Using artificial intelligence to engineer materials’ properties

New system of “strain engineering” can change a material’s optical, electrical, and thermal properties.

Applying just a bit of strain to a piece of semiconductor or other crystalline material can deform the orderly arrangement of atoms in its structure enough to cause dramatic changes in its properties, such as the way it conducts electricity, transmits light, or conducts heat.

Now, a team of researchers at MIT and in Russia and Singapore have found ways to use artificial intelligence to help predict and control these changes, potentially opening up new avenues of research on advanced materials for future high-tech devices.

The findings appear this week in the Proceedings of the National Academy of Sciences, in a paper authored by MIT professor of nuclear science and engineering and of materials science and engineering Ju Li, MIT Principal Research Scientist Ming Dao, and MIT graduate student Zhe Shi, with Evgenii Tsymbalov and Alexander Shapeev at the Skolkovo Institute of Science and Technology in Russia, and Subra Suresh, the Vannevar Bush Professor Emeritus and former dean of engineering at MIT and current president of Nanyang Technological University in Singapore.

Already, based on earlier work at MIT, some degree of elastic strain has been incorporated in some silicon processor chips. Even a 1 percent change in the structure can in some cases improve the speed of the device by 50 percent, by allowing electrons to move through the material faster.

Recent research by Suresh, Dao, and Yang Lu, a former MIT postdoc now at City University of Hong Kong, showed that even diamond, the strongest and hardest material found in nature, can be elastically stretched by as much as 9 percent without failure when it is in the form of [nanometer-sized needles](http://news.mit.edu/2018/bend-stretch-diamond-ultrafine-needles-0419). Li and Yang similarly demonstrated that nanoscale wires of silicon can be stretched purely elastically by more than 15 percent.

These discoveries have opened up new avenues to explore how devices can be fabricated with even more dramatic changes in the materials’ properties.

**Strain made to order**

Unlike other ways of changing a material’s properties, such as chemical doping, which produce a permanent, static change, strain engineering allows properties to be changed on the fly. “Strain is something you can turn on and off dynamically,” Li says.

But the potential of strain-engineered materials has been hampered by the daunting range of possibilities. Strain can be applied in any of six different ways (in three different dimensions, each one of which can produce strain in-and-out or sideways), and with nearly infinite gradations of degree, so the full range of possibilities is impractical to explore simply by trial and error. “It quickly grows to 100 million calculations if we want to map out the entire elastic strain space,” Li says.

That’s where this team’s novel application of machine learning methods comes to the rescue, providing a systematic way of exploring the possibilities and homing in on the appropriate amount and direction of strain to achieve a given set of properties for a particular purpose. “Now we have this very high-accuracy method” that drastically reduces the complexity of the calculations needed, Li says.

“This work is an illustration of how recent advances in seemingly distant fields such as material physics, artificial intelligence, computing, and machine learning can be brought together to advance scientific knowledge that has strong implications for industry application,” Suresh says.

The new method, the researchers say, could open up possibilities for creating materials tuned precisely for electronic, optoelectronic, and photonic devices that could find uses for communications, information processing, and energy applications.

When a small amount of strain is applied to a crystalline material like silicon, its properties can change dramatically; for example, it can shift from blocking electrical current to conducting it freely like a metal. Credit: Frank Shi

The team studied the effects of strain on the bandgap, a key electronic property of semiconductors, in both silicon and diamond. Using their neural network algorithm, they were able to predict with high accuracy how different amounts and orientations of strain would affect the bandgap.

“Tuning” of a bandgap can be a key tool for improving the efficiency of a device, such as a silicon solar cell, by getting it to match more precisely the kind of energy source that it is designed to harness. By fine-tuning its bandgap, for example, it may be possible to make a silicon solar cell that is just as effective at capturing sunlight as its counterparts but is only one-thousandth as thick. In theory, the material “can even change from a semiconductor to a metal, and that would have many applications, if that’s doable in a mass-produced product,” Li says.

While it’s possible in some cases to induce similar changes by other means, such as putting the material in a strong electric field or chemically altering it, those changes tend to have many side effects on the material’s behavior, whereas changing the strain has fewer such side effects. For example, Li explains, an electrostatic field often interferes with the operation of the device because it affects the way electricity flows through it. Changing the strain produces no such interference.

**Diamond’s potential**

Diamond has great potential as a semiconductor material, though it’s still in its infancy compared to silicon technology. “It’s an extreme material, with high carrier mobility,” Li says, referring to the way negative and positive carriers of electric current move freely through diamond. Because of that, diamond could be ideal for some kinds of high-frequency electronic devices and for power electronics.

By some measures, Li says, diamond could potentially perform 100,000 times better than silicon. But it has other limitations, including the fact that nobody has yet figured out a good and scalable way to put diamond layers on a large substrate. The material is also difficult to “dope,” or introduce other atoms into, a key part of semiconductor manufacturing.

By mounting the material in a frame that can be adjusted to change the amount and orientation of the strain, Dao says, “we can have considerable flexibility” in altering its dopant behavior.

Whereas this study focused specifically on the effects of strain on the materials’ bandgap, “the method is generalizable” to other aspects, which affect not only electronic properties but also other properties such as photonic and magnetic behavior, Li says.

From the 1 percent strain now being used in commercial chips, many new applications open up now that this team has shown that strains of nearly 10 percent are possible without fracturing.

“When you get to more than 7 percent strain, you really change a lot in the material,” he says.

“This new method could potentially lead to the design of unprecedented material properties,” Li says. “But much further work will be needed to figure out how to impose the strain and how to scale up the process to do it on 100 million transistors on a chip [and ensure that] none of them can fail.”

“This innovative new work demonstrates potential to significantly accelerate the engineering of exotic electronic properties in ordinary materials via large elastic strains,” says Evan Reed, an associate professor of materials science and engineering at Stanford University, who was not involved in this research. “It sheds light on the opportunities and limitations that nature exhibits for such strain engineering, and it will be of interest to a broad spectrum of researchers working on important technologies.”

news.mit.edu, 01/23/2019

<http://news.mit.edu/2019/vault-faster-more-efficient-cryptocurrency-0124>

# A faster, more efficient cryptocurrency

Design reduces by 99 percent the data users need to join the network and verify transactions.

MIT researchers have developed a new cryptocurrency that drastically reduces the data users need to join the network and verify transactions — by up to 99 percent compared to today’s popular cryptocurrencies. This means a much more scalable network.

Cryptocurrencies, such as the popular Bitcoin, are networks built on the blockchain, a financial ledger formatted in a sequence of individual blocks, each containing transaction data. These networks are decentralized, meaning there are no banks or organizations to manage funds and balances, so users join forces to store and verify the transactions.

But decentralization leads to a scalability problem. To join a cryptocurrency, new users must download and store all transaction data from hundreds of thousands of individual blocks. They must also store these data to use the service and help verify transactions.

This makes the process slow or computationally impractical for some.

In a paper being presented at the Network and Distributed System Security Symposium next month, the MIT researchers introduce Vault, a cryptocurrency that lets users join the network by downloading only a fraction of the total transaction data. It also incorporates techniques that delete empty accounts that take up space, and enables verifications using only the most recent transaction data that are divided and shared across the network, minimizing an individual user’s data storage and processing requirements.

In experiments, Vault reduced the bandwidth for joining its network by 99 percent compared to Bitcoin and 90 percent compared to Ethereum, which is considered one of today’s most efficient cryptocurrencies. Importantly, Vault still ensures that all nodes validate all transactions, providing tight security equal to its existing counterparts.

“Currently there are a lot of cryptocurrencies, but they’re hitting bottlenecks related to joining the system as a new user and to storage. The broad goal here is to enable cryptocurrencies to scale well for more and more users,” says co-author Derek Leung, a graduate student in the Computer Science and Artificial Intelligence Laboratory (CSAIL).

Joining Leung on the paper are CSAIL researchers Yossi Gilad and Nickolai Zeldovich, who is also a professor in the Department of Electrical Engineering and Computer Science (EECS); and recent alumnus Adam Suhl ’18.

**Vaulting over blocks**

Each block in a cryptocurrency network contains a timestamp, its location in the blockchain, and fixed-length string of numbers and letters, called a “hash,” that’s basically the block’s identification. Each new block contains the hash of the previous block in the blockchain. Blocks in Vault also contain up to 10,000 transactions — or 10 megabytes of data — that must all be verified by users. The structure of the blockchain and, in particular, the chain of hashes, ensures that an adversary cannot hack the blocks without detection.

New users join cryptocurrency networks, or “bootstrap,” by downloading all past transaction data to ensure they’re secure and up to date. To join Bitcoin last year, for instance, a user would download 500,000 blocks totaling about 150 gigabytes. Users must also store all account balances to help verify new users and ensure users have enough funds to complete transactions. Storage requirements are becoming substantial, as Bitcoin expands beyond 22 million accounts.

The researchers built their system on top of a new cryptocurrency network called Algorand — invented by Silvio Micali, the Ford Professor of Engineering at MIT — that’s secure, decentralized, and more scalable than other cryptocurrencies.

With traditional cryptocurrencies, users compete to solve equations that validate blocks, with the first to solve the equations receiving funds. As the network scales, this slows down transaction processing times. Algorand uses a “proof-of-stake” concept to more efficiently verify blocks and better enable new users join. For every block, a representative verification “committee” is selected. Users with more money — or stake — in the network have higher probability of being selected. To join the network, users verify each certificate, not every transaction.

But each block holds some key information to validate the certificate immediately ahead of it, meaning new users must start with the first block in the chain, along with its certificate, and sequentially validate each one in order, which can be time-consuming.

To speed things up, the researchers give each new certificate verification information based on a block a few hundred or 1,000 blocks behind it — called a “breadcrumb.” When a new user joins, they match the breadcrumb of an early block to a breadcrumb 1,000 blocks ahead. That breadcrumb can be matched to another breadcrumb 1,000 blocks ahead, and so on.

“The paper title is a pun,” Leung says. “A vault is a place where you can store money, but the blockchain also lets you ‘vault’ over blocks when joining a network. When I’m bootstrapping, I only need a block from way in the past to verify a block way in the future. I can skip over all blocks in between, which saves us a lot of bandwidth.”

**Divide and discard**

To reduce data storage requirements, the researchers designed Vault with a novel “sharding” scheme. The technique divides transaction data into smaller portions — or shards — that it shares across the network, so individual users only have to process small amounts of data to verify transactions.

To implement sharing in a secure way, Vault uses a well-known data structure called a binary Merkle tree. In binary trees, a single top node branches off into two “children” nodes, and those two nodes each break into two children nodes, and so on.

In Merkle trees, the top node contains a single hash, called a root hash. But the tree is constructed from the bottom, up. The tree combines each pair of children hashes along the bottom to form their parent hash. It repeats that process up the tree, assigning a parent node from each pair of children nodes, until it combines everything into the root hash. In cryptocurrencies, the top node contains a hash of a single block. Each bottom node contains a hash that signifies the balance information about one account involved in one transaction in the block. The balance hash and block hash are tied together.

To verify any one transaction, the network combines the two children nodes to get the parent node hash. It repeats that process working up the tree. If the final combined hash matches the root hash of the block, the transaction can be verified. But with traditional cryptocurrencies, users must store the entire tree structure.

With Vault, the researchers divide the Merkle tree into separate shards assigned to separate groups of users. Each user account only ever stores the balances of the accounts in its assigned shard, as well as root hashes. The trick is having all users store one layer of nodes that cuts across the entire Merkle tree. When a user needs to verify a transaction from outside of their shard, they trace a path to that common layer. From that common layer, they can determine the balance of the account outside their shard, and continue validation normally.

“Each shard of the network is responsible for storing a smaller slice of a big data structure, but this small slice allows users to verify transactions from all other parts of network,” Leung says.

Additionally, the researchers designed a novel scheme that recognizes and discards from a user’s assigned shard accounts that have had zero balances for a certain length of time. Other cryptocurrencies keep all empty accounts, which increase data storage requirements while serving no real purpose, as they don’t need verification. When users store account data in Vault, they ignore those old, empty account.

news.mit.edu, 01/16/2019

<http://news.mit.edu/2019/faculty-vinod-vaikuntanathan-0116>

# Fortifying the future of cryptography

Vinod Vaikuntanathan aims to improve encryption in a world with growing applications and evolving adversaries.

As a boy growing up in a small South Indian village, Vinod Vaikuntanathan taught himself calculus by reading books his grandfather left lying around the house. Years later in college, he toiled away in the library studying number theory, which deals with the properties and relationships of numbers, primarily positive integers.

This field of study naturally steered Vaikuntanathan toward what he calls “the most important application of number theory in the modern world”: cryptography.

Today, Vaikuntanathan, a recently tenured associate professor of electrical engineering and computer science at MIT, is using number theory and other mathematical concepts to fortify encryption so it can be used for new applications and stand up to even the toughest adversaries.

One major focus is developing more efficient encryption techniques that can be scaled to do complex computations on large datasets. That means multiple parties can share data while ensuring the data remains private. For example, if researchers could analyze genomic data and patient data together, they may be able to identify key genome sequences associated with diseases. But the information for genomes and patients is kept private by separate entities, so collaboration is difficult. That’s a gap Vaikuntanathan wants to close.

“Data is available everywhere for these purposes, but it lives in silos. Better encryption is a way to ensure privacy yet allow the person holding the encrypted object to get something useful out of it,” Vaikuntanathan says. “Encrypting data and using data for a valuable purpose don’t have to be opposing constraints. You can achieve the best of both worlds sometimes.”

Part of his work also means “future-proofing” cryptography in a world that may soon see the rise of ultrafast quantum computers. Still in their infancy, quantum computers could one day provide breakthroughs in materials science, drug discovery, and artificial intelligence, to name just a few fields. But, because of their incredible speeds, they could also be used to break through most, if not all, today’s toughest cryptography schemes.

“All the existing encryption systems you use over the internet are insecure if you can build quantum computers,” Vaikuntanathan says. “This is something that everyone knows at this point. We need to develop other ways of doing cryptography to secure the internet so it stands strong, even in the face of quantum computers.”

Step by step

Vaikuntanathan’s journey to cryptography, and to MIT, was a step-by-step process of following his academic interests to increasingly larger cities and institutes — and teaching himself along the way.

It started in Neyyattinkara, India, a place so small “you’d find it hard to locate on map,” Vaikuntanathan says. Today, he and his wife still disagree over whether to call it a town or village. But he’s adamant on the latter: “It doesn’t even have a shopping mall — that’s my criteria for calling it a village.”

By age 12, using his grandfather’s old texts, Vaikuntanathan had taught himself an admittedly incomplete understanding of calculus. “It was buggy and error-prone, but as you go along you get better teachers. The best thing one can do is teach oneself these notions, struggle at it — you’ll get it wrong — and then later be enlightened,” he says.

After attending his area’s only high school, Vaikuntanathan, at 15, joined a pre-university program at a technical institute in a nearby bigger city, Trivandrum, about 20 miles away, where he met like-minded classmates. “There weren’t many people who cared about math and science,” he says, “but a few of us banded together and learned advanced math by ourselves.” Of course, there were some disadvantages: “Twenty miles takes an hour in India traffic, on public bus, packed like sardines. Commuting there was not the most pleasant thing in the world.”

Two years later, Vaikuntanathan enrolled in the Indian Institute of Technology (IIT) Madras, in Chennai, a top engineering school in one of the country’s largest cities. “That’s where things started,” Vaikuntanathan says. As he had at his previous institute, Vaikuntanathan formed a “band of brothers” — a trio of students, including himself, who began studying cryptography.

Then, in his junior year, his professor gave him a copy of “Lecture Notes on Cryptography,” about 300 pages of printed-out, compiled notes from a course on cryptography taught at MIT by Shafi Goldwasser and Mihir Bellare. “Our professor gave it to us and said, ‘Go read it and don’t bother me for a year,’” Vaikuntanathan says.

Working with “giants in the field”

Vaikuntanathan sought to carry his interest in cryptography to graduate school. Accepted into MIT and the University of California at Berkeley, Vaikuntanathan recalls asking his father for advice on which to attend: “I showed him pictures from Google of Cambridge, and they’re the dead of winter, with the frozen Charles River; and then Berkeley, which was sunny and full of life. My father said, ‘Go to Berkeley,’ and I said, ‘No, I’m going to MIT.’ It was the obvious choice, because it’s where the giants in the field were.”

One of those giants was Goldwasser, who became a graduate studies advisor: “I learned from her books to begin with, so that was quite fantastic.”

Some of his major MIT work revolved around reinforcing cryptography against the coming age of quantum computing. This involved using lattices, an architecture that uses number theory and hides data inside very complex math problems that even quantum computers can’t crack. His PhD studies culminated in co-inventing lattice-based cryptography schemes; he also developed a toolkit to teach others how to build and modify those schemes, along with former classmate and mentor Chris Peikert and Stanford University’s Craig Gentry.

After earning his PhD, Vaikuntanathan worked briefly as a researcher at IBM and Microsoft. During that time, Gentry invented fully homomorphic encryption, “which changed the world for all of us” working in cryptography, Vaikuntanathan says. But the original model was too computationally expensive to be practical. “For a while, fully homomorphic encryption was nice for cryptography kids to play with, but was useless otherwise,” he says.

In the late 2000s Vaikuntanathan, together with Gentry and Zvika Brakerski of the Weizmann Institute of Science, integrated lattices into fully homomorphic encryption techniques, creating a model that achieved far better security and efficiency. Other researchers have since built on top of the model, which is freely available on Github as BGV (Brakerski-Gentry-Vaikuntanathan). “People have refined that system again and again,” Vaikuntanathan says. “It’s interesting to see how far it’s come in nearly 10 years.”

Vaikuntanathan then taught for a couple years at the University of Toronto. During a summer as a visiting researcher at MIT, however, knew he had to return. “I knew this place had people with boundless energy, creativity, enthusiasm, and optimism,” he says. “It drew me back.”

Vaikuntanathan started teaching at MIT in 2013. Two years ago, he co-founded a startup, Duality Technologies, with Goldwasser and others to develop cryptography technologies that enable users to carry out complex computations and analytics on encrypted data. To Vaikuntanathan, the startup represents how the mathematical concepts he delved into all those years ago have come to fruition.

news.mit.edu, 03/19/2019

<http://news.mit.edu/2019/student-kyle-swanson-computer-science-0319>

# Using machine learning for medical solutions

Master’s student and Marshall Scholar Kyle Swanson uses computer science to help make drug development more efficient.

Pharmaceutical companies spend a lot of time testing potential drugs, and they end up wasting  much of that effort on candidates that don’t pan out. Kyle Swanson wants to change that.

A master’s student in computer science and engineering, Swanson is working on a project that involves feeding a computer information about chemical compounds that have or have not worked as drugs in the past. From this input, the machine “learns” to predict which kinds of new compounds have the most promise as drug candidates, potentially saving money and time otherwise spent on testing. Several prominent companies have already adopted the software as their new model.

“Our model is never going to be perfect … but the hope is that by doing this prediction phase first, the molecules that they actually test in the lab have a much higher chance of being viable drugs,” says Swanson, who graduated from MIT in 2018 with a BS in computer science and engineering, a BS in mathematics, and a minor in music.

Swanson’s overall aim is to use his skills in computer science and machine learning for real-world science applications. He’ll work toward that goal as a Marshall Scholar for the next two years, attending Cambridge University to pursue a pair of master’s degrees, one in mathematical statistics and the other in computational biology.

“I think the ultimate goal is to do something very similar to what I’m doing right now,” he says. “I feel like it’s a great mix of doing interesting computer science research and pushing the field of machine learning forward, while also having practical applications in the sciences.”

**Researcher and survivor**

Swanson’s first experience researching medical applications for machine learning was as an undergraduate in the lab of Regina Barzilay, the Delta Electronics Professor in the Computer Science and Artificial Intelligence Laboratory and the Department of Electrical Engineering and Computer Science. Swanson worked on a system designed to identify the presence of breast cancer from mammogram images. While the original goal of cancer detection proved to be difficult, the tool was successful at a related task. The algorithm is still used to analyze mammogram images, but rather than identifying cancer, it identifies whether patients are at greater risk for cancer, depending on [the density](http://news.mit.edu/2018/AI-identifies-dense-tissue-breast-cancer-mammograms-1016) of their breast tissue.

While he was already interested in machine learning, Swanson entered cancer research for a very personal reason. One day, he noticed he had a little cough, which he attributed to catching a cold from his roommate. But while his roommate’s cough subsided, Swanson’s didn’t. Walking home one night a few weeks later, he found a lump above his collarbone. It turned out to be Hodgkin’s lymphoma.

“My approach is to try and laugh it off as much as possible. I feel like if I were to take it seriously, it would just be so awful I wouldn’t be able to handle it,” Swanson says. “I mean, obviously there were times when I actually was very distraught about the whole thing. … The way I’ve tried to handle it is just to be as positive as possible.”

He asked to join Barzilay’s lab not only because he found her research important, but also because she’d been through a similar scare with breast cancer. He felt that she understood what he was going through. Even now, as he’s working on that pharmaceutical machine learning project, she is still his advisor…”

**KEYWORDS:**

Using artificial intelligence to engineer materials’ properties:

* Bit of strain to semiconductor -> can deform arrangement of atoms -> changes the properties.
* Researchers at MIT, in Russia & Singapore -> ways to use AI to predict and control the changes.
* Already did -> incorporation of elastic strain to silicon CPU chips -> allows electrons to move faster through the material -> gain of performance.
* Strain -> applied in 6 different ways -> 3D & each in-out-sideways) & with nearly infinite gradations of temperature -> impossible to just “try & see”
* Machine learning -> systematic way to explore possibilities to get a given set of properties => very accurate method -> complexity reduced. => Opens possibilities to create materials tuned precisely.
* Diamond -> great as semiconductor cuz electric move freely around -> Ideal for high-frequency electronic devices. => could perform 100k times better than silicon.

A faster, more efficient cryptography

* MIT researchers -> developed a new cryptocurrency -> reduces the data that users need to join network & verify transactions -> up to 99% => much more scalable.
* Cryptocurrencies -> networks built on the blockchain -> these are decentralized -> no banks or organizations for management. => Scalability problem.
* Storage of data can make the process slow or computationally impractical -> Idea is to download a fraction of the total transaction data.
* Each block contains a timestamp, its location and a hash.
* With traditional cryptocurrencies -> users compete to solve equations that validate blocks.
* As the network scales -> processing time slows down => better to use a concept to efficiently verify blocks.
* Here each block contains some key information, and has a new certificate verification info.
* To reduce the storage of data -> new scheme “sharding” -> divide transaction data into smaller pieces.
* Secure way ? binary Merkle tree -> single top node -> two children nodes -> each has two children nodes.
* Top node -> single hash | root hash.
* To verify a transaction -> network combines two children nodes to get the parent one. From bottom to up.

Fortifying the future of cryptography

* Using number theory and other concepts to fortify encryption.
* Goal = more efficient encryption techniques -> scales for complex computations on large datasets. -> multiple parties can share data -> still private.
* Better encryption = ensure privacy while doing something useful from encrypted data.
* In the future, with ultrafast quantum computer -> could be used to go through thoughest encryption algorithms.
* Fully homomorphic encryption -> original = too expensive to be practical -> worked on an algorithm to carry out complex computations on encrypted data.

Using machine learning for medical solutions

* Pharmaceutical companies -> waste a lot of time for testing potential drugs.
* Swanson, CS student work on a project -> feed a computer information about chemical compounds that worked (or not) as drugs.
* With that, machine learns to predict new kinds -> save of money + time.
* 1st experience: medical app to identify breasts cancers based on mammogram images. -> still used but for checking the risks.
* Asked to join Barzilay’s lab cuz she’d been through a similar scare (Swanson found a lump above his collarbone).