An Interview with Thomas Vidick on quantum code cracking

December 15 2014, by Jessica Stoller-Conrad

Thomas Vidick, Assistant Professor of Computing and Mathematical Sciences
Credit: Lance Hayashida/Caltech Marketing and Communications

Quantum computers, looked to as the next generation of computing

technology, are expected to one day vastly outperform conventional computers. Using the laws of quantum mechanics—the physics that governs the behavior of matter and light at the atomic and subatomic scales—these computers will allow us to move and analyze enormous amounts of information with unprecedented speed. Although engineers have yet to actually build such a machine, Assistant Professor of Computing and Mathematical Sciences Thomas Vidick is figuring out how some of the principles of quantum computing can be applied right now, using today's technology.

Originally from Belgium, Vidick received his BS from École Normale Supérieure in Paris in 2007 and his master's degree from Université Paris Diderot, also in 2007. He earned his doctorate from UC Berkeley in 2011. Vidick joined the Division of Engineering and Applied Science at Caltech in June from MIT, where he was a postdoctoral associate.

This fall, he spoke with us about quantum methods for encrypting information, what he's looking forward to at Caltech, and his ongoing search for the best croissants in Los Angeles.

What are your research interests?

My area is quantum computing, so it's the computer science of quantum physics. Classical computers—like the computer on my desk—work based on the laws of classical mechanics. They just manipulate bits and do various operations. However, in the 1970s people started to wonder what kinds of computational processes could be realized using quantum-mechanical systems. They ended up discovering algorithms that in some cases can be more efficient, or that can implement certain tasks that were not possible with classical computers.

In my research, I look at two things. One, what are the kinds of procedures that you can implement more efficiently using quantum

computers? And, two, what kinds of cryptographic systems—ways to encrypt information securely—can you come up with using quantum systems that could be more secure than classical systems? It's all about this exploration of what quantum systems allow us to do that classical systems didn't or wouldn't.

Quantum computers haven't been invented yet, so how do you do this work?

That's a good question, and there are several different answers. Some of my research is very theoretical, and it's just about saying, "If we had a quantum computer, what could we do with it?" We don't have a quantum computer yet because it's very hard to manipulate and control quantum systems on a large scale. But that is just an engineering problem, so what people say is that yes it's very hard, but in 10 years, we'll get to it. And the theory is also very hard, so we might as well get started right now.

That's one answer. But the better answer is that a lot of what I do and a lot of what I'm interested in doesn't require or depend on whether we can actually build a quantum computer or not. For instance, the cryptographic aspects of quantum computing are already being implemented. There are start-ups that already sell quantum cryptographic systems on the Internet because these systems only require the manipulation of very-small-scale quantum systems.

We can also do some computations about properties of quantum-mechanical systems on a classical computer. One branch of my research has to do with how you can come up with classical algorithms for computing the properties of systems that are described by the laws of quantum mechanics. The most natural way to understand the systems would be to have a quantum computer and then use the quantum computer to simulate the evolution of the quantum-mechanical system.

Since we don't have a quantum computer, we have to develop these algorithms using a classical computer and our understanding of the quantum-mechanical system.

Can you give a real-world example of how this work might affect the ways in which an average person uses a computer in the future?

One of the most basic ways that quantum cryptographic tasks are used is to come up with a secret key or passcode to encrypt communication. For instance, the two of us, we trust one another, but we're far away from each other. We want to come up with a secret key—just some sort of passcode that we're going to use to encrypt our communication later. I could dream up the passcode and then tell it to you over the phone, but if someone listens to the line, it's not secure. There might constantly be someone listening in on the line, so there is no passcode procedure to exchange secret keys between us, unless we meet up in person.

However, it is known that if we are able to send quantum messages, then actually we could do it. How this works is that, instead of sending you a passcode of my choice, I would send you a bunch of photons, which are quantum particles, prepared in a completely random state. There is then a whole quantum protocol in which you need to measure the photons, but the main point is that at the end, we'll each be able to extract the exact same passcode: me from the way the photons were prepared, and you from the measurement results. The code will be random, but we'll both know it.

And because of the laws of quantum mechanics, if anyone has been listening on the line—intercepting the photons—we'll be able to tell. The reason for this is that any disturbance of the photon's quantum-mechanical states can be detected from the correlations between the

outcomes of the measurements and the initial state of the photons. This is called an "entropy-disturbance tradeoff"—if the eavesdropper perturbs the photons then the outcome distribution you observe is affected in a way that can be checked. This is a uniquely quantum phenomenon, and

it allows distant parties to establish a secret key or a passcode between them in a perfectly secure way.

How does your work address this?

This system of sending quantum messages was discovered in the '80s, and, as I said before, people are already implementing it. But there is one big drawback to quantum cryptography, and that's that you need quantum equipment to do it—and this quantum equipment tends to be really clunky. It's very hard to come up with a machine that sends photons one by one, and since single photons can be easily lost, it's also hard to make accurate measurements. Also, you need a machine that can generate single photons and a machine that can detect single photons for the message to be secure.

In practice, we don't have such machines. We have these huge clunky machines that can sort of do it, but they're never perfect. My work tries to bypass the need for these machines, with cryptographic protocols and proofs of security that are secure even if you can't make or see the quantum part of the protocol. To do this, we model the quantum equipment just as a black box. So my work has been to try to get these strong proofs of security into a model where we only really trust the interactions we can see in the classical world. It's a proof of security that holds independently of whether the quantum part of the device works in the way that we think it does.

How did you get into this field?

I was doing math originally. I was doing number theory as an undergrad and I liked it a lot. But then I did an internship, and I realized that I couldn't tell anyone why I was asking the questions I was asking. So I thought, "I need a break from this. Whatever I do for my life, I need to know why I'm doing it." The best alternative I could think of was computer science, because it seemed more concrete. And this was when I learned that quantum computing existed—I didn't know before. I think what's most interesting about it is that you're talking about the world—because the world is quantum mechanical. Physics describes the world.

That's what I really like, because from my point of view everything I do is still very theoretical work and I like doing theoretical work. I like the beauty of it. I like the abstractness of it. I like that you have well-posed problems and you can give well-defined answers. But I also like the fact that in the end you are talking about or trying to talk about real-world physics. So every time I think "Why am I doing this?" or "What should I do?" I try to think of how I can connect it to a real, concrete question.

How did you get interested in math and computer science when you were a kid?

My dad was a chemist but he worked as an engineer, and he would come home from work and would bring home different experiments with liquid nitrogen or whatever.

I guess he gave me sort of a scientific mind, but then why did I do math problems? Probably like most people good at math, I was just good at it for some reason and it was just easy. Math is so beautiful when you understand it. Throughout middle school and high school, I just enjoyed

it so much. But then, as I said, eventually I stretched my limits in math a little bit.

What are you excited about in terms of coming to Caltech?

I really like the Computing and Mathematical Sciences department here—it's a young department and it's a small department. For me it's very unique in that there's a very strong group in quantum information—especially the physics side of quantum information, like my neighbor here, John Preskill. Caltech has a very strong group in quantum information and also has a very strong group in computer science. And so, from the point of view of my research, this is just the perfect place.

And then there are the mountains. I love the mountains—they're just beautiful. This is how I abandoned the smoky Paris cafes. I had to think about the mountains. You can't beat the view from my office, and I can go hike up there.

Other than hiking, do you have any hobbies or interests that are outside your research?

I also like to bike up mountains. I did that a lot when I came here, but then I fractured my collarbone while biking. It's almost better now, but I still haven't gotten back on the bike yet. Another thing that is an investment of time—and I'm really worried about that one—is croissant hunting. I really like croissants and chocolates. I'm from Belgium, and Belgium is pretty big on chocolate. I've already been to a lot of famous croissant and chocolate places in L.A., but I haven't found something that has lived up to my standards yet. I haven't done everything though, so I'm open to recommendations.