Science | DOI:10.1145/2447976.2447982 Alex Wright

# Proving Grounds

*Researchers are making headway with one of quantum computing's major theoretical problems: multi-prover interactive proofs.*

As a young computer science master's student at the University of Paris, Orsay, Thomas Vidick began his first research project on the problem that has consumed him ever since: quantum entanglement.

Seven years and one Ph.D. later, Vidick—now a post-doctoral researcher at the Massachusetts Institute of Technology (MIT)—has finally published the culmination of that work. "It took us a while," he says.

In October 2012, Vidick and co-author Tsuyoshi Ito, a researcher at NEC Labs in Princeton, N.J., revealed their long-sought-after result: demonstrating that an important theoretical security protocol, known as a multi-prover interactive proof, could work in a quantum computing environment.

The proof marks the closure of a major unsolved question in computer science—one with important implications for the study of computational complexity and for quantum computing in general.

"It's an outstanding result," says Professor John Watrous of the University of Waterloo, echoing the view of many theoreticians working in the quantum computing field. For the rest of us nonspecialists, however, appreciating why this research matters requires a basic understanding of two conceptually challenging topics: interactive proof systems, and quantum mechanics.

**Multi-prover interactive proof systems limit the ability of independent provers to cheat.**

For the past two decades, interactive proof systems have emerged as a well-established technique in modern cryptography and computer security, by providing a mechanism that allows one machine to confirm another's identity. In the classic interactive proof, a "verifier" with limited computational abilities queries a "prover" that is assumed to have unlimited computing power, but uncertain motives. The verifier issues a challenge to assess the prover's trustworthiness by posing a series of questions, such as asking whether a particular formula can be satisfied. The verifier may then repeat the protocol as many times as necessary to accept or reject the proof.

Researchers have long known that systems with multiple respondents—so-called multi-prover systems—could

PHOTOGRAPH BY PEFOSTUDIOS/ SHUTTERSTOCK.COM

provide more reliable responses than single-prover ones, by forcing the verifier to solicit answers from two or more independent provers. In principle, such proofs should work more efficiently because the provers cannot communicate with each other, thus limiting their ability to cheat.

By way of analogy, consider the case of a married couple, in which one partner is a foreign citizen applying for legal residency in the U.S., while the other is an American citizen. In this scenario, an immigration officer might want to assess whether the couple is really in love or perpetrating a "green card marriage." If the investigator interviews only one member of the couple, there is a reasonable chance that one person might get away with making misleading statements. However, if the investigator interviews both partners separately, then there is a much higher likelihood of spotting any deception—for example, by posing trick questions to catch them on inconsistencies. In much the same way, a proof involving multiple provers ought to yield more reliable results than one relying on a single prover.

In recent years, researchers have also started to explore whether interactive proof systems might work in a quantum computing environment that could, in theory, support exponentially faster algorithms.

Watrous played an important role in the study of quantum single-prover interactive proof systems, contributing to the landmark QIP=PSPACE result, which demonstrated that quantum systems operate in the same bounded space as classical proof systems. "The QIP = PSPACE result answered what was for me the biggest unanswered question about single-prover quantum interactive proof systems," he says. "The multi-prover quantum interactive proof system model, on the other hand, is mostly wide open."

In a quantum computing environment, multi-prover interactive proof systems come with an important wrinkle: the problem of entanglement, or what Albert Einstein once called "spooky action at a distance." When quantum particles interact with each other, they enter a state of co-relation in which they will always behave as if connected, even if they are physically separated.

According to the laws of quantum mechanics, particles have no fixed properties until they are measured. As soon as an observer measures a particle, however, it assumes a fixed state. When quantum particles are entangled, that observation can influence the state of both particles. In theory, then, entangled provers could commingle their answers—posing a risk to the reliability of the proof. What effect might those shared properties have on a multi-prover interactive proof? That is the problem that Ito and Vidick set out to address.

"If the provers can share entanglement, they can use it to generate outcomes that are correlated in a way that is much stronger than anything they could generate using classical means," says Vidick. "The question is then whether they can use these correlations to cheat."

From a quantum computing perspective, "cheating" refers not to any willful act of deception—quantum particles have no ulterior motives, after all—but rather to increasing the likelihood of winning beyond that of a classical proof.

From a mathematical point of view, establishing the effects of entanglement proved extremely challenging. Because quantum computing differs critically from classical computing in its intrinsic reliance on probabilities and interference, it requires a fundamentally new way of approaching computational problems.

"When particles are entangled, their probability distributions can't be treated separately," Vidick explains. "They're really part of a single big distribution. But any mathematical description of that distribution supposes a bird's-eye perspective that no respondent in a multi-prover proof would have. Finding a way to do justice to both the correlation be-

Milestones

# Computer Science Honors, Awards

### SLOAN FOUNDATION ANNOUNCES 2013 RESEARCH FELLOWS

**The Alfred P. Sloan Foundation, which awards grants to support original research and broad-based education related to science, technology, and economic performance, and to improve the quality of American life, recently announced the recipients of the 2013 Sloan Research Fellowships.**

**These 126 early-career scientists and scholars "represent the very best that science has to offer," according to the foundation.**

**Among the recipients are several who are active in computer science fields, including:**

**Nicholas Harvey, University of British Columbia**

**Bjorn Hartmann, University of California, Berkeley**

**Michael Lustig, University of California, Berkeley**

**David James Brumley, Carnegie Mellon University**

**Simha Sethumadhavan, Columbia University**

**Krzysztof Gajos, Harvard University**

**Derek W. Hoeim, University of Illinois, Urbana-Champaign**

**Svetlana Lazebnik, University of Illinois, Urbana-Champaign**

**Fei Sha, University of Southern California**

**Sachin R. Katti, Stanford University**

**Ryan Williams, Stanford University**

**Ruslan Salakhutdinov, University of Toronto**

**Bianca Schroeder, University of Toronto**

**Vinod Vaikuntanathan, University of Toronto**

**For a full listing of 2013 Sloan Research Fellows, see http://www.sloan.org/sloan-research-fellowships/2013-sloan-research-fellows/**

### ANITA JONES RECEIVES AAAS PHILIP HAUGE ABELSON AWARD

**The American Association for the Advancement of Science recently selected Anita Jones, University Professor Emerita of Computer Science at the University of Virginia, to receive the 2012 Philip Hauge Abelson Award.**

**A specialist in computer security systems, Jones was honored for her scientific and technical achievements in computer science; contributions as a mentor, inspiration, and role model for other scientists and engineers; and her lifetime of public service to government, professional institutions, academia, and industry.**

**A member of the National Academy of Engineering (NAE), Jones' previously has received the NAE's Arthur M. Bueche Award, the Department of Defense Award for Distinguished Public Service, a Meritorious Civilian Award from the U.S. Air Force, and the IEEE Founders Medal.**

tween the measurements and the separation of the measurers proved enormously difficult."

Ito and Vidick's proof relies on disguising the questioner's intent by asking multiple questions, thus reducing the likelihood of cheating. That strategy stems from an earlier proof of the classical version of their result by Babai, Fortnow, and Lund in 1991. Their proof demonstrates that quantum entanglement would not allow multiple provers to trick the verifier with an incorrect answer.

Vidick feels the breakthrough insight was, as he puts it, to "stop trying to show that the provers will not be able to use their entanglement to cheat." Instead, they focused their efforts on assessing the entangled provers as a whole. This process involved coming up with a complex set of tools that allowed them to analyze and perform reductions directly with entangled provers, rather than trying to extrapolate results by relating entangled provers to classical provers.

That result has proved an important conceptual breakthrough in the world of quantum interactive proofs. "A major consequence of our work is that it provides a technique to immunize proof systems against the use of entanglement," says Vidick. "This is surprising because we know that sometimes entanglement allows for a large amount of cheating. So it wasn't expected that any classical protocol could be generically resistant against entanglement-based cheating."

Looking ahead, Vidick sees plenty of implications for his work in other research areas. He is particularly excited about the intersection of multi-prover interactive proofs with the world of mathematics, especially functional analysis. He points to Grothendieck's inequality as one example of where he thinks his work could lead to deep extensions, as well as new approximation algorithms for classical problems in learning theory, such as principal component analysis.

While this proof opens up a number of promising new research avenues, the implications for practical computer science applications remain less clear.

"Even if we had quantum computers, it's unlikely that anyone would be able to build one of these systems,"

**Ito and Vidick's proof relies on disguising the questioner's intent by asking multiple questions, thus reducing the likelihood of cheating.**

says Lance Fortnow, professor and chair of the School of Computer Science at Georgia Tech and author of *The Golden Ticket*, a newly available book on the well-known *P* vs. *NP* problem. The computational problems involved would simply be too daunting.

Fortnow believes, however, that the finding may have indirect applications for the larger world of quantum computing. "This result may give us new insights into the limits of quantum entanglement for the purpose of communication between two parties," he says. "It (quantum entanglement) may be even less useful than we expected."

Those implications aside, both quantum and classical interactive proof systems serve primarily as theoretical models for studying complexity theory, particularly around questions of computational efficiency and theoretical cryptography.

"One of the main reasons we study them is because, as theorists, we are drawn to models and notions that we consider to have fundamental importance from a mathematical viewpoint," says Watrous. "The applications would be indirect."

Vidick agrees that multi-prover interactive proofs hold interest primarily for theoretical researchers like himself, although he does see a bright future for more limited applications of quantum cryptography, such as quantum key distribution. "Quantum crypto is really much more powerful than classical crypto, and moreover typically requires only very simple quantum mechanical equipment—much easier to get than a universal quantum computer," says Vidick.

The current generation of quantum protocols relies on single-prover interactive proofs, however—without the messy problem of entanglement. "Entanglement is hard to generate and even more to keep coherently," says Vidick. While there are a few quantum key distribution protocols that rely on entanglement (for example, Ekert 1991), these protocols work by measuring two separated but entangled particles nearly instantaneously—currently a technical impossibility. "I would bet it will be done within 10 years," he says, "but this doesn't mean the use of entanglement will be practical."

From Watrous' perspective, the implications may be largely theoretical, but nonetheless potentially far-reaching. "We are still close to the beginning in terms of understanding this model." C

**Further Reading**


*László Babai, Lance Fortnow, Carsten Lund.*
**Non-Deterministic Exponential Time Has Two-Prover Interactive Protocols.** *Computational Complexity, 1, 1* (1991), 3–40.

*A.K. Ekert*
**Quantum Cryptography Based on Bell's Theorem,** *Physical Review Letters, vol. 67*, no. 6, 5 August 1991, pp. 661–663.

*Tsuyoshi Ito and Thomas Vidick.*
**A multi-prover interactive proof for NEXP sound against entangled provers,** *2012 IEEE 53rd Annual Symposium on Foundations of Computer Science,* September 2012. arXiv:1207.0550v2

*Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous.*
**2010. QIP = PSPACE. In** *Proceedings of the 42nd ACM Symposium on Theory of Computing* **(STOC '10). ACM, New York, NY, USA, 573–582. DOI=10.1145/1806689.1806768 http://doi.acm.org/10.1145/1806689.1806768**

*Julia Kempe, Hirotada Kobayashi, Keiji Matsumoto, Ben Toner, and Thomas Vidick*
**2011. Entangled Games Are Hard to Approximate.** *SIAM J. Comput.* **40, 3 (June 2011), 848-877. DOI=10.1137/090751293 http://dx.doi.org/10.1137/090751293**

*Assaf Naor, Oded Regev, Thomas Vidick*
**2012. Efficient Rounding for the Noncommutative Grothendieck Inequality, to appear in** *Proceedings of the 45nd ACM Symposium on Theory of Computing* **(STOC '13). arXiv:1210.7656v1**


**Alex Wright** is a writer and information architect based in Brooklyn, NY.