

Schrödinger's mousetrap

Part 6: A cryptic response.

**Ilana Goldhaber-Gordon
and David Goldhaber-Gordon**

"Veronique Dubois?"

"And you must be the inspector investigating Rufus Jaeger's death, no? I was wondering if you would want to talk to me." Veronique Dubois and Karl Lister settled themselves into a small lecture room and Lister began his questioning, gently at first.

"I'd like to hear your impressions of Professor Jaeger," he said.

Dubois smiled. "I liked Rufus. You must know by now that not everyone felt that way. Rufus could be quite a ... a shark. But," a contemplative pause, "Rufus and I understood each other." She shook her head and sighed. "I can't believe he's gone, so quickly. You don't really believe it was murder, do you?"

"We have to consider that possibility. Tell me, how often did you see Professor Jaeger?"

"Not very often. We'd attend a few of the same conferences each year, and each time we'd share some meals. But we wouldn't seek each other out. There isn't much to talk about if you can't discuss science."

"You can't discuss science?"

"No. Rufus and I are, were, competitors."

"I see," Lister said, although he didn't really. "Do you talk science with Professor Pruszczyncki?" Phew, he'd pronounced it perfectly.

"Of course," Dubois said condescendingly. "Petra and I are collaborators."

"I see," Lister said again. "And how do you determine who should be a collaborator and who a competitor?"

Dubois looked confused. "I didn't always think of Rufus as a competitor," she said, embarrassed by her bitter tone even as the words left her mouth.

"Did something happen to change your perspective?"

"Early on, I was a bit foolish. I let my excitement betray me, and on a visit to Rufus's lab I shared many ideas. Then an idea I had been nurturing appeared in one of their papers, and I was never acknowledged." During this rush of words, Lister suddenly became conscious of Dubois' accent.

"That must have been frustrating," he said.

"Yes. No. I mean, of course it was frustrating at the time. But it was a relatively cheap lesson. I needed to learn to ... er ... play hardball, and now I know. But, getting back to the present, I think you should see this." Dubois quickly pulled out her palm pilot, stroked in a few commands and thrust it at Lister. "It's a note Wilfred sent to Ludmilla."



Lister read:

hi. I think you should be careful about your relationship with RJ. He is a liar and a cheat. an example. He has just accepted a prize of for the paper on parallel quantum codes which is entirely my work. I realize now that I should have asked the journal from the list of authors

"And how did this message come to be in your hands?" Lister asked.

"As part of my research on quantum cryptography," Dubois responded smoothly. "Both Rufus and I are developing quantum e-mail systems and this message was sent within Rufus's network. To test my techniques, I've been trying to intercept quantum encrypted e-mail messages. You may know that quantum cryptography is supposedly unbreakable. An eavesdropper reveals herself as soon as she attempts to intercept the key..."

"The key?"

"The secret code used to convert a seemingly nonsensical message into the true message. A quantum key is developed collaboratively, between sender and recipient, and it cannot be intercepted without the third party revealing herself."

"Then how..."

"How did I intercept this message? The security of these communications relies on the sender and recipient properly identifying one another. If an eavesdropper could impersonate the recipient, she might fool the sender into developing a quantum key with her, the eavesdropper, rather than with the proper recipient. Which is what I did. So, what do you think of the note?"

"The wording seems a bit strange. Are there words missing?"

Dubois looked at him sharply. "There are, in fact. This is a strange thing: Rufus's net-

work breaks up each 'q-mail' message into 20 or more shorter messages. They construct a new, independent key for every one to two words. From my perspective, this means we rarely intercept the key—or keys, I should say—for an entire message, but only for pieces of it. We can only read messages in fragments. It's unconventional what they are doing, and I had assumed it was because they are new to the quantum-cryptography game. But you know, I wonder. We can read only fragments, and the proper recipient can read only the fragments we miss. Perhaps this breaking up of messages is an extra safeguard to alert against intruders..."

"So Dr Shlomiuka read only the words that are missing from this text?"

"Yes, and whether or not she was aware that she was missing words depends on how her encryption software interfaces with the user."

"I see," Lister scanned the note again.

"It's sad, isn't it?" Dubois clicked her tongue. "Wilfred's been passed over again and again for promotion. And he's been admiring Ludmilla for years and getting nowhere with her. And he clearly has—or had—a grudge against his boss, Rufus. You know, if I were you, I would have a talk with him."

"Yes," Lister said, fingering an imaginary cigarette. "Thanks for the tip."

"My pleasure. Well, if that's all?" Dubois was looking at him expectantly now, suddenly ready to end the discussion. Lister had a nagging feeling that he was missing something, but Dubois' expression discouraged prolonging the conversation.

"Just one more thing, Mi... er, Professor Dubois," Lister said. "What were you doing during the coffee break before the session?"

Dubois smiled at the classic question. "Petra and I were in a study room, discussing our collaboration, as I'm sure she told you." She paused, then looked the inspector in the eye. "Mr Lister, Petra Pruszczyncki and Rufus Jaeger were scientific competitors, not jealous lovers. Theirs was not the sort of competition that provokes murder."

To be continued...

Ilana Goldhaber-Gordon is the author of forthcoming textbook Biochemistry for the Biology Graduate Student. David Goldhaber-Gordon is co-director of the NSF-Stanford-IBM Center for Probing the Nanoscale and is in the Department of Physics, Stanford University, Stanford, California 94305, USA.

Who do you think killed Rufus Jaeger? Catch up on all the evidence and vote for your suspect at
www.nature.com/news/mousetrap