Interview with Silvio Micali

Recipient of the 2012 ACM A.M. Turing Award

Interviewer: Stephen Ibaraki

August 5, 2016

Micali: = Silvio Micali
Ibaraki: = Stephen Ibaraki

Ibaraki: I'm Stephen Ibaraki. It is August 5th, 2016. We are at MIT in the office with Silvio Micali, who is being interviewed for the ACM Turing Award Winners project. Professor Silvio Micali is the 2012 ACM Turing Award recipient and a world-renowned distinguished researcher and professor at MIT.

Thank you, Silvio, for coming in and sharing some of your insights today.

Micali: Thank you, Stephen. It's a real pleasure talking to you.

Ibaraki: Now Silvio, we've got a lot to talk about, and we're going to divide it into portions here. I'm going to first ask about your family background and early life. Then we'll talk about the Turing Award and the research associated with it, followed by your amazing educational journey, which is going to be a lot of fun. Then some broader questions.

First of all, starting with your family background, can you give us your family history? And I'm really also interested in your parents' background as well.

Micali: Alright. I was born in Palermo in Sicily. We were a family of four. My parents, Giovanni and Francesca, and my one-and-a-half-year-younger sister Aurea. It was a traditional family by the standard of the time. My father was the only one who worked outside the home. He was a civil law judge and actually retired as a member of *Corte Suprema di Cassazione* of Italy, and he himself was the son of a lawyer and a judge. So I come from a jurist tradition and a traditional jurist. But somehow, if I step out, it was actually with my father's consent and blessing and actually encouragement.

My father was a Machiavellian realist, but also had incredible enthusiasm for science and engineering. He was convinced they were going to better the world. In fact, he used, "We philosophized long enough. Look where we are. I think it's the time of science and engineering," and of course he wanted to recruit me to the effort. But not knowing much about science and engineering, he had the technique, when I was very young, he showered me with scientific encyclopedias, he brought me chemist's sets. Once when I was 10, we enrolled together in a course by correspondence on electromechanics. We soldered together, we created new compounds on the kitchen table, and etc. But I must say my performance in all this was very mediocre. I think I was more of a theorist than anything else, than an experimentalist.

My mother, totally different. She had no trace of realism whatsoever. Her faith in the ultimate good of humanity was supreme. It took me years and years to somehow shake her very first axiom that somehow very intelligent people are truly good. It took me years to somehow question that. She actually gave me really unconditional love, which I was able to take, but also she had an unconditional confidence in my ability irrespective of evidence and age, which was a little bit harder to take.

So my both parents were very supportive of me and my sister in our studies and they were very loving parents. But also they were very demanding. My father had and still has unbounded amounts of energy. In some sense, right now where we diagnose everything, it would be hyperactive. And his particular kind of hyperactivity came with a demand that everybody else was hyperactive. So if he caught me daydreaming, he'd start to complain. He says, "How is this going to better the world?" My mother instead never thought I was daydreaming. She knew that I was pondering to solve humanity's problem. So in some way, gave us tremendous love, but also they gave me a superego that prevent me to have any rest ever since.

My sister is a statistician. She works for the National Institute of Statistics in Italy. So she also was persuaded to go on the other side of the philosophical side. I must say that I really my love sister. She's a very original thinker. I love her opinions, spending time with her. Unfortunately, by distance, it's a little bit harder to do these days. But otherwise we enjoy our time together whenever we can.

Ibaraki: That's just fascinating. You have this sort of legal background in terms of your family history and your dad excites you in terms of the engineering and the science side, but your mum provides that broader perspective. And you can see that in your work. How does it continue to influence where you're going to go in terms of your future thinking?

Micali: Well, you are right. I really think of it… I really strive to have a… I really love holistic approach to science. Whether I succeed or not, I do not know. But certainly I do not believe very much in compartmentalizing anything, and I think that one thing influences the other. In my thinking, I try not to be caged into any particular discipline.

Ibaraki: You want to share a little bit more about your sibling and their background? You said some statistics and so on. Is there more that you'd like to share?

Micali: Some statistics. Well, so we had essentially very similar background. We essentially… We had very intense parents, and so this is our first bond, first and foremost. I think that is her background and my background that really makes us. But she went totally different and a bit more on the social sciences than I am. In fact, she's interested in statistics of work and then of education. But she really analyzes this from a mathematical way, "How can we model all this and how can we somehow improve both education and work-related policies?" That's what she does. I barely understand what she does.

Ibaraki: I see. It's interesting in terms of your perspective of her work, but does she see the same thing about yours, as sort of a mystery in a way?

Micali: I'm saying that, you know… I believe… I try to convey what I think to my students, to my peers, to my colleagues, but I come from this perspective that I believe family should understand you. Family understands you completely. And I believe that I'm very obscure in discussing what I do with my family because I believe that by osmosis, they should understand it. I'm not sure, but she's said that she has an appreciation of the general directions of what I do, but sometimes I tend to share too many details and I'm sure that I'm foggy and confused, and confusing her. But otherwise, yeah. But somehow the notion of clarity of exposition doesn't apply to family. I think you expect a family should just see you and understand you. When you want to explain the work, that may not the best approach perhaps. So I'm afraid I'm a mystery a little bit to my sister or to my parents in what exactly I do.

Ibaraki: You've described a very rich background in the sense of rich in context and there's diversity there in thinking between your mother and your father. So like a crucible you're incubated. So let's go now into your background, your early background from birth, like when you were born to all the way up and the things that happened to you as you were growing up until you finished high school. If you can describe some of the milestones, some of the things that impacted you or changes in your thinking on this journey of discovery then.

Micali: Alright. Well, my first background and my most important milestone is that I'm Sicilian. Let me discuss what that means to me, the way I see it. Italy is smack in the center of the Mediterranean and has been now a center of many civilizations. The Etruscan one, then the Phoenicians, Greek, Romans, Byzantines, Arabs, and the Normans and the Germans and the French and the Spanish. They were all there and they all left customs, language, architecture, science – the great Archimedes – art, and so on, so forth.

And if you want a complexity that is peculiar to our island… By the way, I believe that all people are complex and each one of us also are multiple personalities. But very often fortunately we have the decency to keep in turn showing up one at a time. In Sicily however, these multiple personalities contend simultaneously for your attention, whatever "you" may be, and never less than seven. So if you have a conversation within three people, actually there are 21 people who are talking and things get very complex very quickly. And all communication is rather indirect because everybody knows the text is only there to convey the subtext, which is the true meaning of what you want to say.

So for me… So it's a very intense exercise. If you're out of practice, out of the island for a while, it takes a while to figure out what is going on in a conversation. But from a cryptographer, there's a balance. You want to have an order because when you want to analyze a protocol, you design a protocol for the way it should be intended to use. But you have to wary of how other people are going to see an exploit from different paths. So if you are accustomed to have these multiple agents concurrently at you at every point in time… I mean let's put it this way – as a Sicilian in cryptography, I think I had an unfair advantage.

Another kind of very early-on influence and another inspiration or advantage is that I spent 12 years in Sicily, then we moved to Rome, and we lived in a town called Agrigento. Once Agrigento, called "Akragas," was a very rich and prosperous Greek city. The poet Pindaros used to say that it was the most splendid city of the mortals. But Pindaros always exaggerates. Another of the inhabitants of Akragas, the philosopher Empedocles, which should be translated a bit more, he used to say that its inhabitants built houses and temples as if we were going to live forever and they ate as if we were going to die the next day. Which by the way I believe it is the intensity that one should approach life with.

So right now, by twist and turns of history, Agrigento's actually one of the poorest cities in Italy, but we still have some remnants, very small parts of old Greek temples. I remember they're really beautiful and I remember as a kid to see so many tourists when travelling was very hard, 50 and odd years ago, that oh, the line-up to see the temples from poor, rich, and from all kinds of background, and really made an impression that if you really do your work well, it will be found beautiful thousands and thousands of years ago. What can be more inspirational than that?

That is really to me a big imprint in me and that also had a particular imprint in my education. This was only elementary schools and two years of middle school. But I had some formidable teachers. I mean my elementary school teacher, Professor Sabia was a phenomenal teacher, perhaps the best teacher I ever had, and I had fabulous teachers. He could command a class with very diverse background, very diverse economic conditions, and lift everybody up, and not only teach but also cause us to have a love of learning. He was really fantastic. And my math teacher in middle school, she couldn't have time to teach much math, but she did more than that. She taught me the love of mathematical thinking.

But also I must say given a glorious past and very challenging economic conditions, Sicily these days is not a place where you want to be an entrepreneur. Certain other things are denied to you when you put everything in education, so you want to have an improvement of yourself which is not finalized to a profession or anything. It's a kind of a moral imperative – "You shall improve yourself, period. If you have nothing else to do, that you should do." And so this particular by some kind of by osmosis I absorbed, and it took me a while… I mean education for education's sake, science for science's sake. Here at MIT, our motto is *Mens et Manus*, "Mind and Hand." It took me a while, years and years after being at MIT to really appreciate how much more science could be when you actually look at application in the context of application and somehow transferring technology and this knowledge to society at large.

So that is my… in Sicily. When we all moved as a family to Rome, and later I acquired a totally new identity, but I kept my old one. In some sense, once a Sicilian you are always a Sicilian, and I kept that as a dual nationality similar to what a citizen from a different ethnic background can have. I believe it's a gift, it's an enrichment. But so I learn to love the Romans. I replaced them with my old Greeks. And the Renaissance. The Renaissance somehow bypassed Sicily. I really learned to love Baroque architecture. Rome has really the real Baroque. And I went to a classical high school, *Liceo Classico Giulio Cesare*. "Julius Caesar High School."

I must say that was a very serious enterprise, and still is. In Italy, you somehow have different high schools for different interests. You can have a scientific high school, you can have a technical high school. If you go to a classical high school, then literature, philosophy, history are supreme, and the math was very little. We had very little. Mostly I had Euclidean geometry, and only because it was Greek I'm sure.

So it was a fantastic period. I believe that… The old saying goes that "Youth is wasted on the young." In fact actually high school is wasted on the high schoolers, because I remember retrospectively, I wish I was a bit more aware of the time, because my mum made me breakfast, I went to school and they start, all these wonderful teachers tell you the best humanity has ever done in all kinds of intellectual activities. You absorb them all, you like some. Mesmerizing, right? So it is not going to happen again. Too bad I was not totally aware.

By the time it ended, it was time to go to college. I had to weigh in what I really wanted to do. I must say that in the first year of high school, this Euclidean geometry really stuck to my mind. This notion that to prove something that happens inside your mind can actually help you to establish truth outside your mind, out there in reality, in whatever is true inside there is actually true out there, and the way in which you can actually develop internally this truth was to me too much to take. So at the time, despite my classical studies, I really decided to enroll in physics instead, going to the university.

Ibaraki: So a really fascinating journey and it was such a classical education, but given a lot of freedom in some aspects of your education. Just for the historical record, maybe we can get some dates. For example, you were born on…?

Micali: Oh. Alright. So I born October 13, '54.

Ibaraki: Then your journey through school, the different sort of milestones from a date standpoint. From your early school to your mid school to high school, do you have any dates that you could insert? It gives the audience a bit of perspective of the time.

Micali: Oh, of the time. Well, you know… Hmm. Now my memory has never been the greatest. So I'm glad that we're keeping at least some record, because if I go to look at this a few years later, I'm going to have already forgotten.

So actually I started the first two… I was born in '54. So I went to a religious elementary school for the first two years. It was… At the time, my father thought it was really the best elementary school there in Agrigento, and actually I had a very fond memory of those nuns. They were very dedicated, teaching us very patient. All of a sudden however, it was becoming slower and slower a woman-only, girl-only elementary school. So there was at some year, I couldn't continue anymore.

At that point, so we went to the public high school. Turns out that the public high school, third, fourth, and fifth elementary school, it was a really an experience. So we had this fabulous teacher, Professor Sabia whom I mentioned, and it was really, really formative. And whatever it was, also it was a notion that we learn together. This guy's job was to allow the people who could do more to do more, but not to forget anybody and bring up everybody, and make sure that everybody collaborated. I must say that that was really a lesson for life. I really believe that science is really a collective enterprise, and even though we did very little science, this notion that it's not an individual uplifting but that it is a collective social effort, I would put it there, third, fourth, and fifth elementary school. Extraordinary teacher.

For the rest, I don't know. Middle school, also there it starts when you are seven, eight, and nine. So that is roughly where you spend there. I remember too it was very rigorous, very much dissecting poetry versus… It was a very intense and also very beautiful. Also in a town in which there are not many ways, economic ways to advance yourself, the profession of a teacher, you are really an authority. You're respected by the entire community. It's a little bit of that fact and really put to me an attention of… That certainly made an impression on me in one way. When I got to the end, I chose an academic career and teaching as a profession. So even that was a very…

But dates, the dates… But we stop elementary schools when we went… When I was 12, I went to Rome, right? Then I was there, I was in high school until I was 18. So one year of middle school was in Rome and then the other five years… the high school in Italy takes five years and I was in this *liceo classico*. So at 18 years old I stopped high school and then went to college, enrolling in physics as I was telling you.

Ibaraki: Silvio, you've got this interesting sort of passage of time in your early education. Were there moments in that time period in your early life where you go, "Wow, that really kind of…" looking back, you think, "Wow, that really shaped me"? Now you mentioned this one very inspiring teacher who also taught you to collaborate but was inclusive and so shapes even today the way you work in science, this sort of collaborative process that gets you to think about the possibilities. Were there other little sort of triggers that happened when you were very young where you think, "You know, that change my life in some aspect"?

Micali: I believe, but I must say… So yes, there was some math problems that somehow I was trying to… But they were very elementary, but I'm saying that I took some effort to prove something myself when I was 12 years old. Very elementary things. But somehow I really felt this love for mathematics. But I'm a very vague memory. And by the way, certain times I can trace, so "Here it is," and certain times I don't trace. I think that actually my keeping a very foggy memory is what actually helps me relate things. So very often, because in the fog, you know… I don't know. Many things are identifiable and things are much more fluent and you can… So I believe I've honestly told you everything that I really remember to be those things, but I have nothing that I can just put a particular…

Well, one thing actually. But again, it was not a moment. It was that I felt that very often my father had a very ethical agenda. He was really totally afraid, never mind what… And I wanted to push the boundary. I think at about say 10 or something, I say, "Daddy, is this legal?" He says, "Why do you want to do that?" I say, "Well, I'm not saying I want to do it. I just want to know, is this legal according to our legal system?" So he says, "You want to do that? You should never do that." "I'm not saying that. I just want to know. So is it legal?" "No." So I sense at that point it was not an opinion *pro veritate*, in favor of truth, but actually a way to influence me. So then I developed various schemes whenever I felt he went into this ethical mode to extract the truth out of him. And as a kid, you depend on your parents to know the truth, and my father wanted to be truthful, but he had also this coloration of ethical behavior. I really felt that I had to be careful in catching which was which.

Somehow that also was in some sense a germ for later work that I did interactive proofs in which you have a very bounded, limited verifier who talks to a very omnipotent prover. The omnipotent prover is somebody who can actually convey and lead you to the truth, but also try to convince you of falsity. Therefore we engage in a game, and how can you, limited as you are, try to put checks on somebody which is actually omnipotent? And so on, so forth. Then I realized that somebody, people say, "Well, how did you think about that model?" So for me, I say, "I knew where it was coming from."

But all these are not moment in time. Are… Is… These are a foggy and necessarily foggy memory. "Necessarily" because I really believe that if things are totally distinct, things are separate. If you want to keep it together, you must blur them a little bit. So my memory is purposely blurred.

Ibaraki: So your memory has these sort of shades that are evolving so that you can do more this associative reasoning.

Micali: Right. I think so. Yes. At least, yeah, I think that's what I'm doing.

Ibaraki: And that's sort of the basis of your genius and all the accomplishments now. We have another question in terms of your family. This is your current family. Can you talk about your current family – your children, your wife, how and where you met, and more that you want to share?

Micali: I'm sure that they want me to share much less than I'm going to share. So I met my wife, my beautiful wife Daniela I should say, here in Cambridge. Somehow… She's actually a legal scholar. She teaches law at Boston University. Interesting enough, her parents, both of them were math teachers at a high school. So in some sense we have totally complementary background, right? She's from a region of Italy, Bari and Puglia, which actually is really the homeland of Romanesque architecture, the pinnacle of Romanesque architecture. Actually when we really understood that we had romantic feeling for one another, when we were actually able to stand alone, sit alone in the Cathedral of Trani, which is a Romanesque cathedral. Absolutely stunning, beautiful. And I must say that at that point, without taking anything away from Daniela, if you are in the Cathedral of Trani, which is not on the coast, it's on a platform on the sea, mesmerizing, it's so moving that you could almost feel in love with anybody. So if you ever want to go and see the Cathedral of Trani, make sure you are in the right company. Okay.

Then we trace actually our movements after getting married and so on, so forth, and we discovered that we actually follow each other very often almost to the same city and the same square by missing each other for a day or so, in Bari, in Gallipoli, in Otranto, and even in Cambridge. Because she took her master from Harvard and then went back for a PhD in Italy. But we avoided to find each other.

But it was meant to be because we met at a party of a common friend from Mexico and somehow I was immediately taken by her. In my excitement, I even misheard her name, so I didn't understand that she was an Italian name. But I addressed her in English, and because her English is so much better than mine, I understood that she was not American but I thought she was British. But any case, she couldn't say a word because despite my inner sense of a signal saying "Stop, stop," I start talking, talking, talking, talking, and I knew that I had to stop. But, well, can I say, at least I must not have made a bad impression. Or at least I was honest – I mean what you see is what you get. I must say that she had the guts to marry me and I'm very, very happy that she did.

We have two wonderful kids, Enrico and Stefano. Stefano is the oldest. They are one and a half years apart. They're both bilingual. Stefano is on the autistic spectrum. He has incredible perfect pitch. He can learn to play an instrument without instructions alone. He can go through a forest or a labyrinth without ever being lost. But certain other things are actually very hard to him. And in those he works with a drive and a perseverance that not even my father could have. So he's really remarkable.

So very optimistic and very energetic, very happy, very happy kid. Right now he's interning for the Boston Duck Tour. I don't know if you know what they are. It's essentially an amphibious vehicle that they show you the town. Then because we are actually a river town, when you plunge into the river and they show it on from the river. He's very happy about that also because this job comes with the side benefit of taking free rides and he was their most enthusiastic customer before. So he's very happy. He's now going to learn cooking and he's enrolling into a baking class. So I'm exercising already in seeing all those pounds coming my way.

My other son, Enrico, he would hate me to say that, so I'm going to say very briefly, not to go back. I think he has really science at heart. More than that, I think he's a theoretician. He would reject the label. He's interested in biology and computer science, but he thinks he wants to start with computer science because he thinks that for computer science, it is easier to go into other fields than the other way around. And he's actually coming to MIT this fall. So whatever I did, I must not have prevented from accepting to coming at MIT.

But besides that, really I'm afraid that I'm hard with both kids, because it is in my genes. I hope they can understand at some point in time that I meant well, but I… But in any case, they would not like me to talk about them, so I better stop here.

Ibaraki: It's interesting you said that your kids will think you're hard on them and you say you're hard on them. Your dad was hard on you. So there's some roots there.

Micali: Yes, yes. It was hard, but again in a very loving way. But my father was a very intense person. Very intense person. And in different ways, so was my mother. In some sense, he couldn't see somebody whom he love, never mind his children, do mistakes, because you had to say the notion that you learn from your own mistake was not at all in the cards. Now I say that I see that despite my conscious efforts, I'm the same.

Ibaraki: Ah, but look what's happened with you. Turing Award winner. I mean, you know…

Micali: Well, I wish my kids the best, but it's going to be their… If I contribute by being hard, then it will be an easy thing. I think… Well, in any case, I hope I'm not too hard.

Ibaraki: Now I'm just going to ask you a couple more questions about your family, but I'm going to reverse it. And that is what do you think amazes… why does your wife think you're amazing and why does she… how would you think she describes you in terms of the things that she thinks are magnificent in you? Then I would say the same thing with your children. Why would they say, "You know what, Silvio is great for these reasons"?

Micali: Let me put my hands down and to say I no claim about what my kids are going to say, because I'm so fearful that I would not… too afraid of their judgment. I think they're going to have good things to say. But somehow I feel that they hold me to a higher bar than they should, and I'm not sure I measure up to the bar.

And Daniela actually understands me, but in fact I actually believe that I could describe and subject her to hear about my work, but I also love to hear about her work. She's a very original thinker. Somehow she struggles because she thinks that in law, scholarship rather than originality should be prized. So she always feels that she should be doing things differently. Instead I love, I find very insightful everything she says. I have a little bit of experience in law by the distance to appreciate the insight into society and really the law itself that she has. So she's really a true companion. She's also a very severe judge because she can tell me, "Silvio, you are wrong. You are doing this wrong," and so on, so forth. To be told that you're wrong, you can bypass it if you think that people don't understand you. But if you start, if you accept the notion that they do understand you *and* you are wrong, then you might be wrong, okay? So I really value her opinion and try reluctantly to change myself in the way she suggest I do change.

Ibaraki: So Silvio, we'll now talk about your Turing Award and some aspects of your research. Now when did you hear about this extraordinary honor, that is the recipient of the Turing Award, which is widely regarded as the Nobel Prize in computing? And this was the 2012 Turing Award. How did you feel at the time? What was the reaction of your colleagues, your family, and more?

Micali: Well, okay. First of all, how it happened, it was the weekend before President's Day. And actually we organized a ski trip with Shafi's family, so it was very purely coincidental. Think about that, because we won the Turing Award together. So the telephone rang and Dr. Ready informed me of that. And how do I feel? How did I feel? I felt good. First of all, I must say I was always very proud of the work, so it naturally felt good that it was recognized. But I also felt good that it was the work together with Shafi got recognized, because the two of us really worked very intensively together in overcoming many rejections, difficulties, and different hurdles. We were trying to put together a theory of interaction, and to interact, you need to be two at least, right? So I really felt it was only proper, in fact frosting on the cake that we got it together.

And I must say that other people's reaction was, happy to say, very positive, very enthusiastic, and very moving to see this, particularly from the colleagues and all. We are, in theoretical computer science, a very closely-knit community, so I put a premium on what the colleagues say. And I'd say my mother wasn't surprised. She always knew… But they were very happy, my parents too. So I felt it was very good. So part certainly of… a side effect of this thing, of this award, is that it make you feel good, and feeling good, you are better at thinking and doing research, teaching, at everything else.

Ibaraki: Well, it's interesting. You talk about you're on this sort of ski trip or you're planning with Shafi and you happen to get the announcement when you're playing together in essence as a sort of consequence. Then you talk about how it impacts other parts of your life. So let's talk about that. This question is about how has the Turing Award impacted your work, your influence, and your thinking?

Micali: Alright. Work first. So okay. I really believe that to do scientific work, or all kinds of work, you need somehow… or in particular scientific work, you need two components – (a) you want to seek for universal truth and try to push the boundary, and the other thing is that you want to get universal recognition. I don't think that these are in conflict, by the way, because the moment in which a scientist no longer cares about what society thinks of him, that's a very dangerous place to be. On the other side, if you want to have social recognition, the easiest way is to work on very well-defined problems that society already agrees they should be solved, so you do much more conservative work. There is tension between these two things. My hope is that if the Turing Award has at least momentarily calmed down my desire for social recognition, it gives me more freedom to explore more and to go more on a limb in my research. I think that is going to be the impact that I expect and hope for my work.

The other thing is about the influence. Well, so influence on outside the field? Outside the field I think absolutely it's a very visible award, and like other major awards, it makes you visible to people actually outside of your field and that actually you become essentially an ambassador of your field. You can certainly use this recognition and influence for the common good, because very often you may be contacted by somebody who wants to have a pointer in the right direction of computer science, so you can make some connection and suggest links and be useful that way. I hope I will… It's a responsibility. It's an opportunity. I hope I will use it well.

For inside the field, I don't believe much has changed or should change in the sense that computer scientists, in particular theoretical computer scientists knew about my work with Shafi anyway. And in a true scientific field, there is no such thing like proof by authority. I mean, so I expect, and it's actually good to be so, that our colleagues will continue to judge us with very high standards. From this point of view, there is no influence at all.

So the influence on me, I was saying, is good because it's a boost, right? Not an immediate boost, though sometimes you have a down time first. But then eventually some boost. And if you have more energy, you can put it to work with renewed enthusiasm in your research and scientific activity. So I think that will be the influence that it is going to have on me in particular.

Ibaraki: Reflecting upon your answer and your work, it sounds like there's problems out there that people have worked on a long time, and that's true of all researchers – they have to work on these sort of classic or old problems and they gain you a lot of recognition for that. But what I'm hearing is, is that getting the Turing Award allows you to work on more novel issues, or maybe things that would be considered risky for a young researcher.

Micali: Absolutely.

Ibaraki: It gives you freedom.

Micali: Yes, yes.

Ibaraki: Can you talk more about that freedom?

Micali: Absolutely. By the way, I want to make a premise of my co-recipients of the Turing Award, they didn't get it for mulling old problems. They all were path breakers in their own ways in different directions. But I mean you really need freedom because the danger is really to be incarcerated in a kind of an established way of thinking, and very often the older the problem you solve, the more recognition you get. How can it be? These old problems, at some point you need to solve them too, but I think we should put always a premium in grabbing new aspects of reality and bring them into very scientific analysis. And I believe it is possible to do more. We don't even know what we are going to grab yet. So if you ask me, "What is next going to be understood?" I do not know. But I believe that's how we really measure improvements, in which we extend scientific thinking to parts of life that we didn't think were amendable to rational analysis. And this, it comes either for an innate sense of self-entitlement – good thing to have – or sometimes if you… like in the case of your award, when you're given some self-entitlement by… You're given entitlement by others rather. Then you feel free to say, "You know what? I'm going to push a little bit more the envelopes in another direction," and you allow yourself to do that.

So I think that is a very constant part of this. I think you need both to have really a viable scientific community. But my preference is always for the magmatic stage in which you are about to comprehend a new part and you start creating structure where there was no structure whatsoever. That's my sweet spot for me, but everybody has his own sweet spots, or their own sweet spots, and we should be welcoming all of them. So we need really a full approach to make science.

Ibaraki: Again, based on your response on this question about the Turing Award impact in your work but also your influence and your thinking, you have this really notable achievement. It's a part of the historical record forever. As a result, it gives you this influence, but it also allows you to meet people in other fields who will recognize this achievement. And there have been some studies to indicate that the more diverse your people clusters, the more innovative you're going to be, it's just going to help in your research. Have you found that?

Micali: Absolutely! In fact, let me tell you that it's not easy to receive an award, or at least it's not easy for me. Because first, initially you're happy. Then, at least in my case, you are depressed. And the third thing is that finally, at some point is all, you have to interact with other people who go to the… An award, receiving an award, there is an occasion which you are brought together. At that point you get back the enthusiasm again, because all of a sudden you find people that have a totally different interest from you and you start having very good person-to-person conversation about "What are your goals? What is your field?" Then you see how they approach it, how they want to go about it to achieve their goal, and it's very inspiring I must say. You feel really energized about this. So that is the third stage. Also now you've made a few friends, and if you need a bit some help, you know whom to ask. So yes, this aspect is really there and I really believe really adds the personal touch, the personal level that is very important.

Ibaraki: Let's see if we can extrapolate a little bit further. So you won this historical achievement, the Turing Award, plus many other historical achievements, but we're sort of focusing on that, the Turing Award, right now. How do you think now this changes your life goals? Or has it? You know, your big overarching life goals that you want to achieve and sort of the process that you've achieved them, can you talk more about that?

Micali: I can, but I'm going to be very brief because my life goals haven't changed and I don't expect them to change. My life goal is to understand the world and being understood. Somehow I'm convinced that they are very related if not identical. The way I'm going to go about trying to achieve these goals is very simple too. It's by supreme confidence and by supreme doubt. You need both. That's the best I… That's what I will… what I have done. And barring emergencies, that's what I plan to continue doing.

Ibaraki: You mention supreme confidence and supreme doubt. Is the doubt what causes you to ask questions and continue to think about problems? What is the doubt? How does that help?

Micali: Oh. Well, so let's deal with confidence first. I mean if you have no confidence, you cannot do things of value. Somehow you must bootstrap yourself. You somehow say, you must say, "I can do it." If you don't have that, then it's very hard to start any journey.

However, the doubt is very important, but I mean perhaps in a different sense. Because if you don't have any doubt in your ability of achieving the goal you set up for yourself, then you're not pushing yourself hard enough. So what you want to do is to get the perfect spot in which to say, "Will I be able to?" and things. Anyways, that's the level I wish to operate.

Ibaraki: I think there's sort of some profound statements that you put out, and just fascinating. You know, I've done these interviews for a long time, since the 1980s, and I've done over a thousand, and you come out with these amazing statements that I think will live forever. So just very deep thought.

Let's talk more about the work that led to the Turing Award. You wrote, or co-wrote one of the most influential papers in computing science on "Probabilistic Encryption" as a graduate student in 1983. Can you tell us what led you to write this paper, sort of the journey and the process?

Micali: Yeah. The main process, so the process is two engines, if you want. One is fearlessness and the other one is luck. Let me put the emphasis on luck, because my Roman ancestors would call it a *condicio sine qua non*, which is "that without which nothing." I mean without luck, nothing of importance can ever be achieved. And we were lucky, Shafi and I. Our first luck was we were together and attending a course of Manuel Blum, which is a fantastic teacher, and the course was on computational number theory. And the last three lectures, only the last three lectures were about cryptography.

We were in a fantastic position in time and space. Then a question was raised towards the end of the course, which was almost put up there to say, “Can you play mental poker?” So not to play poker with physical cards in front of you and so on, so forth, but what if you want to play over the Internet by exchanging messages? Well, when in such a case, “Sure, I’ll play poker with you, but do you mind if I do the dealing?” Right?

Then that was the luck. The fearlessness comes that all of a sudden, this is so exciting a thing that Shafi and I decided, “Oh, that’s what we should be doing.” You know, first-year graduate student. It turns out that we eventually succeeded in doing it, but it took us a decade. Fortunately… Which “fortunately” is another form of “fortune.” Essentially we didn’t have the… able to size the magnitude of the problem we were against, which made therefore much more eager to attack problem, and that was very fortunate.

Then however we realized that to solve the problem, we really needed to have a better way to encrypt. Even before the dealing, before anything else, you need to encrypt somehow the cards. The dealing, let’s put it aside for a while, but how do you encrypt the cards? And encryption until that point was deterministic. If you have one message, there is only one possible encryption for it. So what prevents essentially somebody to understand the ciphertext is the messages are long. I mean technically should say “have enough entropy.” Because if you are to guess a long message exactly, it’s very hard, so you don’t quite know, given the encryption, what the underlying cleartext was. But when we’re talking about poker, we are talking about 52 cards, so there is not long messages. In some sense, you know *a priori* it’s one of these 52. So we decided on actually to say, “You know what? Let’s make it even harder, the problem. How about if you want to encrypt only zero-one?”

So this making the problem harder actually made it simpler. That was actually really our luck to try to make it harder, because once if you want to go zero-one, there is only one possible way of skinning the cat. Namely you must have necessarily a probabilistic way of encrypting. So every bit, zero for instance, must have myriads of ways to… myriads of encryption of zeros in which without any secret, you just randomly pick one of them and that’s what you send. Point two, no matter which one somebody has picked, to each one of them you should be able to reconstruct zero, because otherwise you have no understanding from people. And the third thing is that, from an adversary who just sees passing by a random encryption of a bit, he doesn’t know which, if it’s zero or one, he cannot have better than 50-50 ability to understand if it means zero or one without the secret. Because assuming that the only message is yes or no and you understand say 75% of the time that “Oh, it’s a yes,” then you can really do damage as an adversary. So it should not be 75, it should not be 60, it should not be 51, it should not be 50.5. It should be 50 plus epsilon, with a very, very, very, very small epsilon.

So we decided that that's what we should be focusing on. To tell you the truth, at this point we had the definition, at least for this elementary message space, what a good encryption ought to be like. If you have the right definition, you are half done. Then there is the rest of the work. We had to do that too. So the rest of the work was say, "Okay. Now I know the properties. Now I must find some way to implement this property." I mean that's already very good, to come up with the right definition. But then you must implement it.

Then we had another strike of luck. That is a luck that somehow maybe favors the young or at least favors me, and that is ignorance. Ignorance is a form of luck because what you want to do is that… when you know a lot… Think about a big haystack. So you put all your knowledge into this big pile that you cannot somehow juggle in your mind at the same time. But what you are needing and looking for is the needle, which is how do you implement, given the immensity of whatever you know, the right way to implement the three properties that I just said? But if you are ignorant, if you have very few pieces of straw, to find the needle is easy. And you must be lucky because first of all the needle has to be among this straw. But it was.

I remember we had a course. It was the first course ever done at Berkeley – I don't know about the rest of the country – on computation, on number theory. Number theory is one of the oldest subjects of mathematics, but before the computer. And we analyzed a few problems. Essentially we said, "We bet it's one of these." So when you over there, when you say, "We found this problem," which was called the quadratic residuosity, which means over the integers, if you ask it say, "Is 25 a square?" sure it is – five times five is 25, is a square. "Is nine a square?" Sure – three squared is equal to nine. But when you want to modular arithmetic, so you want to take something and you square it, and then skipping various details, then divide it by *n*, if you want to take a number modulo *n*, and then look at the remainders, very hard to figure out if something is a square or not. But turns out that if you know the prime factorization of *n* – which is something not easy to compute, but you can take two primes and multiply them, and by definition, you know that prime factorization was this number – then figuring out if something is a square is very easy. But when somebody is… a number is relatively prime with *n*, never mind the precise definition, and as Jacobi symbol 1, never mind the 2, then for somebody who does not have the prime factorization of *n*, it seemed to us as very hard to figure out if something is square modulo *n* or not.

So we felt to say, "Well, it's so simple, it's so beautiful, so stark, it ought to be true." So we start asking around a few experts that we have in the department in number theory, say, "Do you know how to figure out if a number is a square modulo *n* if you don't know the factorization of *n*?" They say, "Well, not really, not really, not really." That's it. So at that point, we say, "It has to be true." We went on the record and say, "That's how we found our cryptographic system, based on quadratic residuosity."

That's another advantage of somebody who has no reputation to defend, because we were first-year graduate student. If we were wrong, nothing would happen. Assume we have a reputation, then you are much more conservative. But we were in that spirit. But we landed in an island, we had a look around. There seemed to be nobody around. When we put a flag, this island now is the kingdom of Silvio and Shafi. So things were done like, more or less was an act like this.

Tell you the truth, so that was our example, and then we… If the example would have been proved false in 2-3 months, maybe the whole thing would have collapsed. But they didn't. In fact, for all that they know, it could be true now. So we were lucky enough. But at this point, even if it's found false, we found many other ways to implement the process we want. It wouldn't matter. So it was really a stroke of good luck.

At some point, I must say I always respect luck, but after that there is work. So we had somehow to prove things. Having guessed that was hard, and so we had to develop what turns out to be the notion of computational indistinguishability, the hybrid argument, and random self-reducibility. All kinds of techniques that would become the bread and butter of future cryptography, but we did it then on that particular example because we wanted to play mental poker. That is really roughly what went on back then.

Ibaraki: That's sort of an amazing process, and the fact that you were so young allows you to take these leaps and take chances as somebody later in their career would not have done. But because of that, you've created a foundational piece of research that is the basis for much of what we have today. It's amazing that you had this confidence as well to take this journey and to start formulating how this is going to come about.

Let's delve into this in a little bit more detail now. Can you tell us a little bit more about what's behind your approach to the simulation paradigm?

Micali: The simulation paradigm. Okay. Maybe it's just best to explain by relaying a rather personal episode.

I was a teenager. I forget, as usual in my foggy memory, where exactly… what number was after one, but I was at that stage is a very vulnerable stage. Somehow I went through a stage of solipsism that I'm sure all of us have gone through. Namely the feeling that the world outside doesn't exist and it's only you who are concocting this reality which is rather virtual than real.

And okay, so everybody goes through that. I had a bit more acute perhaps episode of this because I was convinced that the world didn't exist and I was dreaming up, that I start acting consequently. So if the world doesn't exist, why should I go to school? First step. Okay. So I take one day, two day off. But again, if it don't really exist, why should I get out of my pajamas, right? I mean… Fast-forward a little bit, my mother really got very worried. I remember she sat down with me on my bed and tried to put some sense into me and to say, "Silvio, what is this? It's nonsense. The world exists. I exist. I'm talking to you." And say, "Ah, so you don't exist. You're a fruit of my imagination. I let you say whatever you're saying right now."

At the end, good thing is that I got out of it. The other good thing is that I was able to put this personal experience and transform it into science. In particular, the simulation paradigm. What is the simulation paradigm? It is a technique to prove that the amount of information conveyed in interaction is bounded. It's a way – right? – to bound. So if we talk back and forth, "What are we doing?" you can just say, "How much information has actually leaked?" And assume that in cryptography you want to avoid this leakage. You want to compress as much as you can.

Let me give you an example. In cryptography… Once I saw a beautiful vignette. It was two dogs typing on a keyboard, and one dog tells the other, "Over the Internet, nobody knows you're a dog." It's wonderful. But over the Internet, in fact what distinguishes you in a cryptographic interaction from anybody else is that you know one secret key. That's what makes you. Therefore any interaction with you, you take a message, you take your secret key, you concoct a response, you send it. Take another message, you look up your secret key, compute the response, send it. Therefore, every response that you send out there has been processed using your secret key. Think of it in some sense, the secret key, some distorted image of it is embedded in this response, because you have looked up your secret key, you've used, you manipulated it to compute the damn thing. So perhaps some part of the secret key is now embedded in the response that you send. And you send a lot of responses during a protocol. Think about every response like projecting over a wall the shadow of your secret key, because it's in there. You have used it. So if you don't use the secret key, you're not doing anything. But if you use it, you might betray you. So you have a projected view of my secret key on the wall. When I send you another message, you have another angle projected again on the wall. Then a third angle and so on, so forth. Then perhaps from all these angles, why shouldn't my secret become clear? How can we guarantee that this does not happen?

But assume that I could do the following. Say, "Stephen, if you guess four bits say – the right bits, but four is a small number of bits – if you get these right bits, then you can in your own mind concoct a conversation with me which is identical to the conversation that you and I right now are having. Assume you have this ability. Well, how much information can I possibly convey to you about my secret key?" Well, so it's no more than four bits, because if you can guess these four bits and you can simulate me completely, whatever I'm helping you dream about my secret bits is only these four bits.

Essentially that is a way… So in some sense what happened is that this old notion, that idea that stuck that it was impossible to distinguish reality from virtual reality, from a product of your mind, now has become essentially our best tool to bound the measure or the amount of the knowledge leaked into an interaction. And that is really fundamental for cryptography because you want to use the key, secret key, but making sure that a minimum, a bare minimum of it is leaked.

Ibaraki: It's a really interesting concept that formed the basis of what we do today, and pretty profound with this approach. Now let's continue this sort of journey. Can you now describe your notions around encryption security, such as semantic security, indistinguishability, and how these measures must be met for schemes to provide security across the wide range of cryptography applications?

Micali: Let me start with semantic security, okay? I'm a very excitable person and say I make an exclamation. Say I say, "Mamma mia!" say 10% of the time. Start with this, which is believable in my case. So if somebody says, "Silvio's spoken. What does he say?" "Well, he says, 'Mamma mia!' " and you'd be right 10% of the time, just because the only information you have, "Silvio's spoken. 'Mamma mia!' is what he said."

Let's assume now that not only I've spoken but actually I've encrypted what I said and shipped it over the Internet. Now you have two things – not only the notion "Silvio's spoken" but also you actually have the ciphertext of what he has said. So if you decide to ignore the ciphertext, you can still say, "Well, it's 'Mamma mia!' " you will be right 10% no matter what, like before. But now if you cryptanalyze the ciphertext, then perhaps your 10%, you can improve it. You can improve it to 15, right? But if you cannot improve it to 15, not to 14, not to 13, not to 13.1, but only to 10.000001, then the encryption is secure, because in some sense the presence of the ability to analyze an encryption doesn't give you any advantage on what you knew beforehand about me anyway. Right? That's the idea of semantic security in a nutshell.

So the other, indistinguishability, is a totally different approach. By the way, so if somebody says about semantic security, could rant and rave and say, "What does this mean? This models me. Like what am I? A machine who finishes sentences with some probability? I'm a human! I have free will!" Whatever. So you say, "Okay. Good. Calm down. I have a definition for you too." And the definition is computational indistinguishability.

What is this? This is an operational rather than ontological way of distinguishing two things. Let me, before I get into that, just in case I make it wrong, to give some kind of inkling on what it means, let me paraphrase it. Assume you go to a jewelry store and you see there is a beautiful diamond priced at $1 million appropriately. You say, "Wow, wow. This is a wonderful diamond. Is it really worth a million dollars?" "Oh, by all means. Look at the purity, look at this. This is a million-dollar diamond." Then your eye got caught on another diamond that looks remarkably similar, but it's priced at $1. So you say, "Well, this other diamond, it's just $1." "So that is a fake diamond." But it looks the same. He goes, "Oh, of course it looks the same." "But if you operate with a microscope, it will look the same?" "Oh, of course it will look the same." "If I put…" I don't know what you put to the diamonds. "If you put it in the microwave and you shake it up, will it react in the same way?" "Oh, of course it will look the same. Listen, no matter what you do, no matter what experiment you can do whose result you can see in your lifetime" – results of experiments that we don't see when the sun is cold, we don't care about those – "anything you could do in a lifetime, it would look at the same." You say, "Really? Well, do you mind giving me two of the $1 type of diamonds?" because at that point, in what sense are they different?

So if I have no experiment that I could do or my children or the children of the children can do that separates two things, shouldn't I be coherent, rationally coherent and say that maybe I should identify the two things? That is computational indistinguishability.

So technically how you want to put it, assume that I give to you two messages, different messages, *m* and *m*-prime. Two different messages. And I'm going to consider all the possible encryption of *m*. Remember there is zillions of them and we select one of them to encrypt, right? Then I have all the zillions of encryptions of *m*-prime, and they ought to be separate because from each one of them, you can reconstruct *m* and *m*-prime. So it is "What can a distinguisher of encryption ought to be?" Well, in essence, ought to be an algorithm, some procedure that, given an encryption of *m* or *m*-prime, try to tell you which is which. In essence, it's a procedure that given an encryption spits out zero-one. And you can interpret zero as to say, "Oh, I guess it's from *m*," and you can interpret one and say, "Oh, this is from *m*-prime." This procedure had to be polynomial time, which is a technical term, means "Ought to finish and give you an answer within your lifetime or within the lifetime of humanity." Okay? Fair enough.

So now I can define a probability, which is the following. Take a random encryption of *m*, feed it to this procedure, and look how many times it outputs zero. This probability is well defined. It may be hard to compute, but… So I take an encryption of *m* at random, I feed it to the distinguisher, and I look how many times therefore we got probability output zero and overall the possible coin tosses for selecting the encryption of all the possible coin tosses of the procedure. This probability, I want to call it P-zero.

Now let's consider another probability. I take a random encryption of *m*-prime, I ask the distinguisher and I see what is the probability that again it outputs at zero. How you want to call this probability which is also well defined? How about calling it P-zero prime? That makes sense. Good.

So encryption to these two messages are indistinguishable if P-zero is equal to P-zero prime plus or minus epsilon, 0.000001. And I say, "Okay, that's a formal definition, but what does it mean?" It means the following. Assume that you are writing to the general-in-chief and somebody says, "Sir, we have found the enemy has sent an encryption. And good news, our intelligence tells us that it's either an encryption of *m* or an encryption of *m*-prime." "Very good. Let's distinguish it, which one of the two of them." "Very good, sir. We have a wonderful distinguisher, which in a month is going to tell us zero or one." "Very good. Run it and come back and report."

So you feed this encryption to it, the distinguisher huffs and puffs, and after a month spits out zero. You go back to the general, say, "Sir, up to report that the encryption, the distinguisher has said zero." He says, "Well, what do I care?" because essentially the distinguisher says zero with the same odds whether the encryption was of *m* or was of *m*-prime. The fact that after the answer, you give me the answer, I don't know what to do with the answer. In fact, I only have wasted a month of electricity to run the damn machine. Therefore really the encryption is good. And it turns out that now there are two ways of right describing a thing, one in which you endow the probability space with an intrinsic probability distribution – say Silvio says an exclamation with probability 10% or something like this – and another one is probability less… there is no probability on the message space at all. Now the question is "Well, that looks good, that looks good. Which one should I use?" And as is usual in life when things are good/good, they are the same. So these two notions are actually the same notion, and therefore it gives you some confidence that the right notion of secure encryption is conveyed.

By the way, at this point we also know a third and fourth way that also coincide with these two ones. So we believe now it's a very robust notion.

Ibaraki: I see. It kind of reminds me of – and I think you've talked about this – Turing coming up with the sort of computational theory of computing and then you have lambda calculus doing this sort of stuff in recursive functions, and really they're talking about the same thing.

Micali: It is exactly the same thing. At the time in which people wanted to define what was computation, there were many ways of recursive functions. There were lambda calculus. And he said, "I believe that what is computable is the recursive function," says "I believe it is lambda calculus." And Turing says, "Well, I believe it's whatever a Turing machine can do." And turns out we don't have to decide, because they're all equivalent. So that is really the way in which math is kind enough to tell us we are done. We can relax. We have our definition.

Ibaraki: Yeah. There's almost like a poetry and it's almost music in the universe when you have these different approaches really talking about the same thing.

Micali: Exactly, yes.

Ibaraki: And it further substantiates the quality in the foundational pillar that you created through this work.

So to this next question then. Overall – and I think we've already touched upon this, but we're going to expand on this – how did your work revolutionize the study of cryptography and then lay the foundation for the theory of cryptographic security?

Micali: Well, so let's try to see what was the status of the art before. The status of the art before was essentially mostly heuristics. Very good heuristics, very complicated, well thought out heuristics. But essentially you tried to construct a cryptosystem, you tried to poke, to kick the tires, you look for holes, you don't find any bugs. Then you go through a list of bugs. I try this, I try this, I try this. Therefore at some point you had to stop and you say, "Well, I stop and I believe that there is no other bug. Among all the possible infinitely many others, this stuff is solid." So of course it's a very heuristic process and there is somehow no proof.

Instead, the work that Shafi and I have done is rather different. It says, "We want to prove." So we want to prove… And what is the proof? We want to prove that the ability in a cryptographic system to gain any understanding about the message should be equivalent to factoring numbers.

Okay, factoring numbers we already mentioned. Let me say one more time. So 21 factorized is three times seven. Three is prime, seven is prime. Three times seven is 21. So if I take a very large 1,000-bit prime or 10,000-bit prime and another very large 10,000-bit prime, I can still multiply them by hand even. It'd take me some time. But once I get to the product, good luck to figure to what *p* and *q* are, the two primes really are. So that is the problem of factorization, and it's a very hard problem in computation. Perhaps we could do something with quantum computing. Perhaps not. The jury is still out. But in any case, certainly that's something that has baffled the minds of generations of mathematicians.

So what we want to do is to say we want to prove these two problems are equivalent. And what do I mean that it is equivalent? Assume that you have found a way to generate some understanding from messages encrypted in the cryptosystem. Really? Then I can make money on you in the following sense. Somebody says, "Hey, I have here a 10,000-bit composite number, product of two primes. Can you factor those?" "Oh, I certainly can. But however I want to be paid for my effort, so I want a million dollars for factoring the things." "Deal." "Good."

What I do now is I take this number, which is a number. It has nothing to do with messages, with encryption, anything else. I massage it around. I create an encryption scheme out of it. I take some message myself. I encrypt it. Then I call you. "Stephen. Hey. I know that you can understand something about messages in this. Could you understand something of this?" And he says, "By the way, to the word of your good efforts, I give you $1, because I want to make money on…" And you say, "Okay, yes," and you give me the answer, "I believe that this message you've done this." Very good. I keep on doing this two, three, four, say a thousand times. Now you give me a thousand answers, whatever it is. Then by theorem, I take these thousand answers and with a little bit more computation, I spit out the primes that multiply in the original challenge that I was given and I collect my million dollars.

So essentially it is that no matter what you can think you can understand, any procedure, you can very quickly convert it in a procedure that factors primes and nothing else, so it becomes a pure mathematical problem. And tell you the truth, if somebody understands something about encryption, my conversation, encrypted conversation because he knows how to factor, he deserves to understand what I'm saying.

So that is the thing. That's the new type. Nowadays you want to have this type of proofs, of equivalence between a pure mathematical problem and the proper understanding. And this of course comes with another thing, which is the effort in which you want to model. What does it mean to have an understanding? That's a vague concept, right? First of all, you must model this so that in a way which is uncontroversial, it becomes that you have understood something. Then you want to have an explicit procedure that says any way to get this understanding is actually a disguised way of factoring numbers. That is a totally different approach that we go from a heuristic approach, in which it tells you that there is no other shortcut, there is no other bug because whatever is a bug, then whoever finds this bug also found a very effective, efficient way of factoring numbers.

Ibaraki: Yeah. I guess by extension then, you take this heuristic approach and it's really dependent on a particular kind of technology that exists at the time. If you have a mathematical theoretical base to it and there's a direct connection between the technique and that math modeling, then no matter the platform, it still should work.

Micali: Right.

Ibaraki: So you just mentioned quantum computing. What are the implications of quantum computing? Will the work extend to quantum computing?

Micali: Well, if quantum computing is right, then based on factoring, it cannot extend by definition. But we could do the same type of reduction. Factoring is kind of easy to describe, so if you don't mind, I stick to factoring for now. But otherwise, there are other ways, other type of problems to create a cryptosystem from in which you still have this equivalence but the problem you're equivalent to quantum computing has no claim at least as yet about it. Then therefore… But the old approach essentially is to go from a heuristic to a proof of equivalence, I think it was proof of equivalence of a sort. So that is how the game has been changed, that's how the game is played now. If you don't have such a proof of equivalence, people don't take you seriously, any cryptosystem. You must have at least for one meaty problem, you have to be equivalent to it.

Ibaraki: Yeah. Well, again just amazing what you've accomplished, and sometimes… I think earlier you said that working with Shafi was a bit like working with seven people or something.

Micali: Oh! Yes, yes. Shafi is an honorary Sicilian.

Ibaraki: Let's continue on this journey now. Can you talk more about your work with knowledge complexity and zero-knowledge proofs?

Micali: Okay. Zero-knowledge proofs. If you look at the proof, say, "What is a proof?" Well, a proof is many things. A proof can be beautiful. A proof can be inspiring. A proof can be boring. But no matter what, at the very end of the day, it must convince that something is true. It has to convey the verity of some information. So zero-knowledge proof actually essentially are a way to separate verification, so you can verify the proof is correct, from information, so from the knowledge. You can verify whether the proof is correct but have no idea about why.

For instance, sticking back to this analogy about factoring – if you already used once, might as well use twice. Of course I can have a number that is product of two primes. I can take two primes and multiple them together or I can take three primes – right? who's counting? – and multiply them together. When I ask you… So therefore, you can ask. They say, "How many primes does this number have?" and I can say, "Three." They go, "Well, this is a declarative statement. Do you mind proving it?" One way to prove it is of course to exhibit prime number one, prime number two, prime number three. What do you do? First you inspect that each one of them is prime. Then you multiple them together and see the product is the number that you had in mind. That is a proof. But that's a proof that conveys much more knowledge. It doesn't only convey that the number is product of three primes. It conveys exactly why it's product of… It gives you the three primes. It gives you all the information you want.

A zero-knowledge proof is a way to somehow allow you to prove a statement in a very convincing way without letting any inkling of why this is so. It's like if the sky opens up and somebody says, "This is number is product of three primes." Okay, when you believe it but you don't say more than this, you are actually convinced of it, but you don't get any more information than the statement itself. That is what a zero-knowledge proof is. So essentially our intuitive notion of a proof, let's say the two of them are together, they can actually be totally separated.

Then you say, "But who cares about giving proofs?" but that actually is the same technology that then you use to marriage correctness and privacy. It is very easy… For instance, in an election, you want an election to be correct and private, right? But to have an election correct, and say everybody tells me, digitally sign or sign what the vote is, I go on public TV and I say, "I have 17 noes and 14 yeses. The 'no' win. Okay?" They say, "Yeah, right." And when everybody sees the digitally signed piece of paper by the participants, they say, "This is true," but there is no privacy whatsoever. On the other side, if I want to have privacy, I can just say, "What's your vote?" "Yes." "What's your vote?" "Yes." And when I go here, "Ladies and gentleman, there are 17 noes and 14 yeses. The 'no' win," it will be a revolution. How do I know?

The notion that you can have your cake and eat it too can be done. You can actually have both correctness and privacy. So you can actually be sure of the correctness of the tally and you have no idea about who voted for whom, and you have them both. So you can see that this actually is kind of an important development in cryptographic theory, because people love privacy and people love correctness too. If you can actually have both, that's a good deal.

Ibaraki: It's interesting. You talk about this zero-knowledge proof and you have the sort of prover and verifier. I guess there's implications to that because you can extend that to have maybe a multi-prover situation and verifier, and that extends to maybe multi protocols on the Internet or something like that, user protocols. So I guess this question then is can you talk more about the implications of this work and how it extends to other domains? You gave an example in terms of elections, but can you talk more about that?

Micali: Well, okay. Let me… Okay. So implication of zero-knowledge stuff. Let me give you two ways. One is more mundane than the other. Let's talk about the dating.

Now dating is a very complex social operation, because you'd like to know, if you like a person, whether the other person likes you too. That's quintessentially human, right? But on the other side, can you imagine that I go to someone and say, "I want you to know that on a scale of 1 to 10, I love you 10. How much do you love me?" When, heaven forbid, the answer comes "2," I'm quite embarrassed.

So you don't do that. But assume that instead you have a date app in which two people can actually say… they can input the grade to the other, and it could be a 10 and a 4 or it could be a 10 and a 10 or any other combination. And the following thing happens. If they both like each other 10, a green light comes up. And otherwise, red light and no other information. Then I have nothing to lose, because I can put my true feeling and true grade to the other person, and if I'm not going to be reciprocated, it's never going to be known by anybody what my grade was.

In this way, what I really believe is that this field of zero-knowledge in security in this sense essentially allows for more interaction, allows us to safely interact with somebody. Safely from a correctness point of view, safely from a private point of view. We will interact more and no less. So we are going to be perhaps even more human and facilitate human interaction that way. That would be one social app.

If you want to have other things, so right now for instance, with Shafi again and Ron Rivest, who was here an inventor of public-key cryptography… Another wonderful colleague here, in fact the one who hired me and Shafi. So the few of us come up with a way of doing digital signatures. Digital signatures are much better than the scribbles we are accustomed to, because they're digital and they're really unforgeable. Only you can sign, but everybody can verify. Let's assume that this is true, that it's a magic number that somehow allows you, but only you can produce but everybody else can verify you produce and therefore certifies that you agree a given sentence.

This digital signatures used to be that you want to prove that you cannot forge the digital signature of a message of your choice, because otherwise our wonderful Mr. Gates, who has been really a great computer scientist or really done a lot to society and donated a lot of his billions to society, let's assume he has still a few billions left. Then I could say, if I can forge Bill Gates' signature of "Bill owes Silvio a billion dollars," then the digital signature would be no good.

But then if you think about it, you don't want… the inability to forge a message from scratch is very little, because if I receive a signature of somebody that they owe me 10 bucks, this I could not forge beforehand, but once I see the signature, can I transform it into a signature that same person owes me a hundred bucks, a thousand bucks? I multiply to how much he wants. The digital signature would be in danger also. And if you fast-forward this, then perhaps what you could do is that you can somehow get a bunch of signatures from somebody. Perhaps you can ask this person, “Could you please sign this? Could you please sign this? Could you please sign this?” And then from all these answers, you’re able to sign something that he has not agreed yet to sign, something new. If this happens, I want to declare the digital signature bad also.

Then you can just say, “Oh, this is overly pessimistic. Who in his own head is going to digitally sign messages that somebody else concocts for him?” You say, “Really? That’s exactly what a notary public does.” You go to a notary public and he’s not going to say, “I refuse.” Your business is you sign copies of a document. So in a notary public situation, you actually can implement this attack of being asked and being forced to digitally sign something, but then you want to make sure that no matter of what you have not yet signed, it’s still unforgeable.

If you think about it, you want that the process of digital signature should be unlearnable. So that’s what it is that zero-knowledge means, is that you can sign as much as you want, but you want to prove that you are not gaining any knowledge sufficient to forge the digital signature of a new message. That’s for instance where it comes from. And nowadays, all self-respecting signatures are of this type. They satisfy this type of condition. It has actually a variety of applications.

Ibaraki: I’m just thinking of the… You know there was the financial crisis in 2007 and the government now is assessing the portfolios of banks.

Micali: Oh, right.

Ibaraki: So I guess an extension is analyzing all the banks.

Micali: Absolutely. I have a wonderful colleague and friend, Andrew Lo of a business school here at MIT. He actually had exactly this idea. So congratulations to you, that is a great idea. He had in mind to say, “Hey, let’s have a way to do it,” when you want to do the stress test. Banks usually don’t want to reveal their positions, their portfolio, because they say it’s a secret. Or if you’re a trader, you don’t want to say what you are going to do. But the government may have actually legit interest to know that there is not something wrong going on. Therefore if you actually give a zero-knowledge proof that, even not disclosing your portfolio, you are complying with all rules and regulations, the government is happy and you’re happy too. So that gives also another approach to… It’s another way to play the game. It’s another dimension to play as a society that we didn’t have before.

And in fact, very often… let me extrapolate a little bit more, even allow me to be generic here, to say very often we have insider trading or other activities that somehow you punish, that are punishable by law. There shall be no insider trading. Why? Because if you utilize this information you should not have even though it was imperative that you had it but you misuse it, then you go to jail. But wouldn't it be better rather than punishing people to use these cryptographic and zero-knowledge protocol to say, "Hey, I can verify whatever I want to verify, but I don't have information. So don't ask me, because I cannot. I would love to inside trade, but I can't." Then forget forbidding and we go into another realm in which we are to say prevent from the very beginning. And very often in fighting crime, everybody wants to prevent. But then at the end, everybody is forced to… somehow to punish. Instead the best way, you really can prevent.

Ibaraki: Again, it's just so profound, all the applications, and especially because the proliferation of the Internet. We got about 3.2 billion people now using the Internet. There's over 7 billion people using mobile… Or 7 billion mobile phones, not 7 billion using them at this stage. But you know that at some point everybody's going to be connected, so privacy and correctness is a big issue at the same time, and you're enabling all of that with the work that you're doing. So it's just…

Micali: Yes, very true. By the way, I must say some of these techniques become very inexpensive computation, some are more expensive, but the trick is going to be to inject them where it matters so that they put an undue burden of complexity of the whole thing and keep us working safely and interact much more than we would otherwise.

Ibaraki: You talk about the application of this zero-knowledge proof and you gave really great examples that we can sort of relate too, because it's everyday. And the Internet is just a proliferation of individuals. Obviously you want to maintain security and secrecy and privacy, and yet have correctness as well. So I guess the applications then are somewhat unlimited and only left to the imagination because of this foundation that you led.

Now on this next question, I ask about some of the practical problems associated with the protection of data from being viewed or modified because of the Internet and the transactions that occur. But I think you've answered that because you talked about digital signatures.

Micali: Perfect. Well, no need to.

Ibaraki: Yes. There is also the impact of your work on computation complexity. Can you talk about that?

Micali: Well, sure. Computational complexity aims to study how much time and space, how much resources do you need to accomplish a given computational task? Because it used to be that people felt, "Oh, this is computable. We are done." But then you see we start realizing, "Hey, this algorithm will take forever, so in what sense is this computable? And then how long, how fast can I get this problem? And which problems have fast solutions?" so on, so forth. So one of the ways in which I somehow could have made a contribution is that aid in the notion of an efficient proof. Because traditionally the notion of a proof has nothing to do with efficiency. It has only something to do with truth, because you have a theorem, never mind how long the proof is. At the end, if the theorem is correct and the proof clicks, it's verified correct, done.

But somehow I argued and something I made the case that somehow intrinsically in a proof system, there are two agents, the prover and the verifier. We insist that the verifier is lazy. Why? Because the moment in which to verify a proof takes you as long as to find the proof yourself in the first place, all mathematicians would be out a job, because who needs them anymore? Writing the proofs were so long. So intrinsic, even without realizing it, there is always this notion that verification ought to be much easier than proving. So somehow, however, I really say, "Well, actually this ought to be nice. Can we actually force this? How do we really define proofs this way?" and that is one thing.

Another thing is that another type of proofs that are called computationally sound proofs, these are proofs that are always very efficient, both to prove and to verify, but allow to have… to prove anything, both true statement and false statement. Then I would say if you prove a false statement and true statement together is an anathema. What is good, such a proof?

Well, slow down, because now we can use computational complexity in the following way. Assume that I can prove in the old fashioned way that even though good-looking proofs of wrong statements exist, the time it takes to find even one of them is exponentially big, then that is good enough. Because even though they both exist, proofs good and bad, if I give you a proof, you say, "Well, one of two things. Either the universe has worked for billions and billions of years to concoct all this or the theorem is true, which one you believe?" Well, I think in some sense the latter, not the first. So we can use complexity to bypass Gödel's incompleteness theorem and to have complete completeness and consistency in a mathematical theory. I believe that is another thing.

Another thing is pseudorandom number generation. In some sense in complexity theory now, randomness helps to speed up computation, so it became very important to figure out if probabilistic computing is really much more powerful than deterministic computing. Pseudorandom number generation is a way somehow to prove if there is any extra help, extra advantage that randomness gives you is perhaps much smaller than we thought before.

So all this could be… Complexity theory's a wonderful field and I believe complexity allows to describe a lot of the things that goes on, not only in computation, in the universe. And at least in these particular few sectors, what I've has intersected with complexity theory.

Ibaraki: In many ways, the people in the complexity area have really sort of taken off with your work, and it's even got them to think of new ways of doing things, maybe even introduced new sort of strains of research in this complexity theory.

Micali: That is true. But it's also true that I used complexity theory instruments and tools and conceptual tools in my own work. So everything is interrelated. We are in a soup together.

Ibaraki: Yeah. And there's this idea of pseudodeterministic algorithms.

Micali: Yes.

Ibaraki: So it has its practical applications for people in the software field as well.

Micali: Yes.

Ibaraki: What about some of the other practical applications and implications of work influencing our daily lives? Let's assume now there's people listening to this podcast, or I should say this video, and they may be executives and they're not really into the nitty-gritty or the technical side and they want to see… And we've talked about some of the practical applications. But are there others that you can talk about, the practical applications that we see every day in our lives?

Micali: Well, let me venture to say that most practical aspects people meet in their life about cryptography are passwords, because passwords allow you to identify to a main server say where you store your data and give you permission to act on your data, and so on, so forth. But passwords essentially, classically is a shared string that I know and the server knows. So it's very dangerous because if I just give you my password in the clear, an enemy could listen and then can impersonate me to the server.

But even if you bypass this and you try to make this disappear, then you are led to another thing. Namely, the server ought to know my password at least. In that, many application is no good because for those people who are like me that once they memorize a password, they use as much as they can, I have plenty of applications in which I use the same password. So in principle, anybody on the other side of each one of these applications could impersonate me in the other application, which they shouldn't.

It turns out that there is another desideratum that you want in a password. That is somehow that if I use the password to log in say to a server, I don't want any trace that I have actually logged in. If for instance I sign by giving you the datum, which I digitally sign the datum, this works as a password, then you can prove to somebody else, "Silvio's digital signature that he accesses this database." Instead, from this point of view, the perfect password is really a zero-knowledge proof, because essentially I'm going to tell a server, say, "Hey, here's the statement of a theorem." Its a theorem that I concocted myself. I take two large primes, multiply them together, and say, "Theorem, this number product of two primes. Anybody who can prove it to you, that's me. I authorize/sign anything you want to access my data, to wire money on my behalf, do anything you want."

But so then how do I authenticate the work? I just gave you a zero-knowledge proof that the theorem is true. If you think about it, by Definition A you are convinced that it's me, the proof is correct, but the proof is zero-knowledge, which means that you don't learn anything, any more but the statement of the theorem. Therefore could you be able to prove it to somebody else? No. Because if the guy clams up and says, "This number is the product of three primes," and now you believe it, that doesn't allow you to prove it to somebody else, because… Right? That is very…

So this zero-knowledge proof systems are really the perfect password. That is the simplest, most straightforward application that somebody can actually encounter in real life.

Ibaraki: All of us when we open up our wallets and there's all these cards and things in there, is there an example do you think of the things we carry on, that we carry with us in our everyday lives that uses fundamentally zero-knowledge proofs?

Micali: Well, some of these zero-knowledge proofs are used behind the curtains to implement really secure authentication, and yes, over the Internet and things. But I want also for your audience to appreciate one thing, which is very hard but I'm going to try to do it.

What people apply is not a theorem but a theory. You apply… Sometimes you are lucky. You take a zero-knowledge proof, straightforward it's a perfect password system. But the application, what you apply is a theory, is a way of thinking, is a way so that all the protocols that are actually deployed are actually complying with all these other objects, even though they do not correspond to a theorem. Strange enough, we demand about science, or particularly mathematics, the application of a theorem. That is wrong. We really have to look about the application of a theory. It's a bit more abstract, but it's more historically true.

Ibaraki: Well, Silvio you've taken us on this journey of discovery to the process of getting a Turing Award and the underlying research that led ultimately to the Turing Award, which is a lifetime achievement of outstanding accomplishment. But yet you're still quite young and you have much more to do. But there's other aspects of your research. Can you talk about that, some of the other research that you've done and their lasting impact, and some of the lessons that you want to share from that research?

Micali: Well, in terms of other research, I've been doing research on distributed computation, some on mechanism design. But perhaps I think the poor listener has had enough of technical things.

In terms of lessons, I think that to a young a person, I would really strong advise to focus on the problems that motivate you. Really you, you, you. Because I believe that any creative process, whether it is artistic or scientific, ultimately at the core of it there is a desire to solve an emotional problem that we carry within us from when we were very young. So we will never tire to solve that problem because we want to solve that problem, and that I think you're going to get an energy forever because you don't need any further motivation. That's the way to go, to really focus on what you care about deep down.

The other lesson I'll say technically would be try to generalize those examples that really motivate you. Because the real-life examples are actually messy. There are a lot of details, and all these abundance of details blind us now. So what you have to do is to somehow back up from the picture until you have a clear and neater picture, generalizing the picture. Then you back up, back up, back up until you actually drive yourself to a corner. Because a cornered man is a very dangerous man, so you can, as a scientist, be very dangerous if you put yourself in a corner. Because at that point, (a) you fight for your life, and (b) the problem is either so simple, simplified that you can solve it, or somehow it becomes impossible. Either way, I think you win. And who needs partial victories? So I really believe that generalizing and try to go for the heart of the problem and drag yourself into a corner, that is the right way to go.

Ibaraki: What I'm hearing you say then is that, rather than focusing too much on specifics, you start looking at "What are the foundations of problems?" in essence or "What's the underlying reasoning behind it that can apply to many circumstances?" If you keep going to sort of the simpler and simpler and simpler context of what it is, you get to a basic truth, a fundamental truth of the world, of science, of nature. And sometimes you may fail in that, but even in failing, you'll learn a lot. But in solving it, of course you advance the world in some scientific way.

Micali: Yeah, that too. But I must say, but actually the problem sounds simple. Like for instance if you take the problem of encryption, I'm sure that if somebody else would have asked the question, say, "How do I encrypt a single bit?" we would have tried to do… would have this probabilistic encryption developed earlier? So somehow try generalizing and simplifying. Sometimes I've been trying to apply this principle, but sometimes I've not been able to, and I really realize that somebody else actually made progress by just bucking up and asking a simpler, starker question. Because we think much, much better when you are on a verge of a cliff and then there is a stark contrast between everything else and then a thing becomes clear. Sometimes it becomes clear that this problem is impossible. But occasionally it is not.

Ibaraki: How many times do you think you've applied this process? And when did it first start, at what age do you think, this idea of backing up, backing up, backing up to get to this foundation?

Micali: I think that actually that very early on, anytime that I had actually a problem that gave me some grief, the only way I knew how to solve was really to assimilate it and break it down into… isolate its core components and things. Again, with my bad memory, I cannot… But ever since I remember, if a problem gives me grief, that's what I do.

Ibaraki: Perhaps your solipsism when you were a child is really getting back to a fundamental truth.

Micali: Right, right, right, right.

Ibaraki: Let's now switch a little bit and let's talk about your current research interests. What are they? What are your current interests?

Micali: Well, right now I think it is implementing a public ledger. That means something like… I don't know if you know about Bitcoin, that type of work, in which somehow we live in a very distributed world, each one of us sees various chunks of reality. I can see some transactions, I can see some payments, you can see different transactions, different payments, everybody. So therefore we need to have somehow a common knowledge understanding. We need to say, "Well, never mind. Many things have happened, but we must officially declare *these* are the ones that, as a humanity, we agree have happened."

This public ledger is a way essentially to do that. That would give a lot of clarity in humanity. I believe that there are some wonderful approaches out there to solve a problem. I mean they are very much admiring all these very clever ideas. But a clever idea and a beautiful idea doesn't mean that is the idea that is really sufficient. I believe that there is more to do and I'd like to try, if I can contribute something to this creation of a public ledger.

Ibaraki: It's interesting, this idea about a public ledger, and I guess then you get to this application through blockchain and you have the R3 Consortium. I guess it's over 40 banks now are working with this, and there's other groups.

Hyperledger, another group working. So the application of these public ledgers through blockchain, do you see other sort of applications of that, in how it can be used and then the implications of that use?

Micali: I think other people better than me already have argued for public ledger. Essentially not only you want to find something which is common knowledge but also something that is tamper-proof, so that you cannot change the history of what has happened after you declare an official history. So this is going to add all kinds of clarities to everything.

For instance, assume we have a startup. When you do, when you say, "Hey, if you write this piece of software, I give you a thousand shares." Right? I have a piece of paper, I sign it. Somebody else will say, "Oh, if you do this for me, I give you 500 shares," and I sign up. Then suddenly, "Okay, we won the lottery. Google, Microsoft, whatever wants to acquire the company." Then the first thing I want to know, what are the liabilities of one's shares, right? And that is very hard to figure out, even in good faith, and somebody else come up with a piece of paper later which is a disaster. It puts a wrench into lawyers' engines and so on, so forth. But essentially if you have actually a single history which in all these events have been embedded in this history, then it becomes much clearer what the hell has happened, so that is going to really simplify a lot of humanity.

Let's put it this way. Over the web right now you can find everything. The truth, true facts, false facts. They're all… Good luck. But very often, never mind "true" in the mathematical sense, you really want to say, "Hey, what are really the facts that have really happened in this social sense?" and you'd love to go to the web and have some very clear sense of this. I think that we should invest in society more in order to do that. But the way currently this is done, I believe at least… I'm getting the zest of what various approaches are, but I have not yet found an approach that I'm very happy with. Therefore I'd like to try my hand and try to see if I can improve this aspect, because I do believe that this is going to play a fundamental role in society in improving our lives.

Ibaraki: I guess the implications are everything.

Micali: Everything from cryptocurrencies to smart contracts to titles, passing it on. Very often even in Third World country, a lot of progress cannot be done because you have to bribe everybody to have a title to something you really own. If it's already a public domain, you don't need to bribe anybody else. It could be anti-corruption. It could be a lot of stuff.

Ibaraki: It's just fascinating. I know that earlier you had some interest in mechanism design. Is that work continuing?

Micali: Yeah, that work is continuing. But I believe it is a beautiful discipline. I'm very late. In a fair world, I should have learned about mechanism design many years ago, but I didn't. I was lucky to find people who guide me through it, because when you come as a later age without a proper education, you're very naïve and so you need some help to somehow… And I got some help, some wonderful friends and colleagues. And I continue to do so. Right now I like to work on some aspects of mechanism design.

But I must say, I must confess that I'm a monomaniac and it's very hard. I'm very obsessive and it's very hard to obsess about two things. So right now it's public ledger that's top of my imagination and that's what I want to do.

Ibaraki: So public ledger is your focus. Just for the purpose of this archive, because we've mentioned mechanism design, maybe you can just define it so that…

Micali: Oh. Design, it's a very cool aspect. Assume that you are a decision maker and you want to take some decision on behalf of the people of society. You are a mayor of a city, you are a chair of a department, and you want somehow for instance maximize your people's happiness. So you go into a new building, so "What would you like?" Say, "I'd like a low floor, sun exposure. I'd like a more square space." Therefore if you knew what people wanted, you could as a dictator somehow optimize collective happiness. Not the happiness of everybody but collective happiness.

But very often as a decision maker, you are the last one to know what your people want. Therefore you have to ask them, "What do you want?" But then it's very tricky because the moment in which you ask them what they want, people say, "Ooh. Stephen is going to ask what I want. I guess he has this algorithm to allocate resources after I tell him what I want. So let me try to declare false things, because I know which direction he wants to go, so to tilt the outcome that is going to be chosen by Stephen in my favor." So you don't get the truth by asking. You get what people want to hear because they think they're going to influence your final decision. Therefore you get garbage-in, garbage-out, if you get bad ideas. Therefore what you want to do is to find a way to elicit correct or correct-enough information from the players who are the ones who really know what they want so that you can actually take some intelligent and socially optimal or good enough decisions, good enough outcome.

So that's… And it's a fascinating field.

Ibaraki: Well, you talk now about some of your current research interests, now with a focus on public ledger. How about your future research interests? Now I'm talking further out into the future. What are the things that "You know, I'm kind of intrigued by that. It sounds really interesting"?

Micali: Stephen, you ask very pointed questions. I'm going to answer this question as if we have contract that you don't ask me how, okay? Because something that really interests me but I have very, very little knowledge about and only very limited things to show is the brain. I believe the brain is a fascinating subject and I believe the brain has a lot to do with computation, because somehow computation has to be part of our brain. There are colleagues and friends like Les Valiant who has given much more thought than I have, actually for years. And I believe that is something that… not so much that perhaps I will explore, but maybe in another life I might have explored. Maybe I will explore it too.

So far I've only, with another colleague of mine, Nir Shavit, and two students, wonderful students, Gelashvili and Allen-Zhu of ours, we actually found a brain-plausible algorithm for compressing information. It is an algorithm for compressing information that has some biological basis to be credible to happen in the brain. Is it right? Is that what happens in the brain? That's somewhat less relevant. But the important thing is to start talking about these things so that we get into the habit of reasoning in this way, and eventually we will find out a lot of things about the brain. I'm very bullish about our ability to understand it and actually to bear computational tools in doing so. It will require a lot of collaboration with biologists and computer scientists, and very great mutual understanding. But I think that is a great, great direction to go.

Ibaraki: Penrose takes this approach about the brain and he talks about maybe sort of the quantum aspects of it, microtubules, and there's some other characteristic we don't know and that creates consciousness. Then you have Daniel Dennett, *Consciousness Explained*, and he's maybe trying to give it more a rational… I shouldn't say "rational" or "irrational," but more of a mechanistic kind of point of view on maybe how things come about. Or Descartes with his mind-body philosophical point of view. In your approach to this, it sounds like you're taking a computational…

Micali: Absolutely.

Ibaraki: …"There's a process of what makes us who we are."

Micali: Right, right. Because at the end, I must say nobody wants to be called a… most people don't want to be called a computational machine. But never mind what they want to be called. We do actually compute quite a bit.

So my interest… The brain is a lot of things, as you say. But one aspect of things, the one that particularly fascinates me is to say, "Hey, we must process information. We must store information. Where do we store it? How do we retrieve it? How fast can we do it?" In fact actually, at least what I was saying before, how we compress it. So there ought to be even some compression going on. That's at least this little paper that we wrote, it was trying to figure out "How do we compress?"

So if you take… Right now we're taking a video of this interview. Well, there are many more pixels in me right now than are in the video. And if we take a lower-resolution camera, there would be even less pixels, right? And if you take a toy camera, even less pixels. But nonetheless, we'd be able to recognize each other from this compression. Why? Because it's a good compression if you somehow maintain angles between vectors and relative magnitudes of vectors. And so at the end, we must do something like this, right? Otherwise where do we store it? We have a tremendous amount of neurons, but at the same time it's a finite number and there is a lot of pixels about reality out there. So we cannot possibly store. We must somehow do… What is really the mechanism for doing so? That is… The brain is about many things, but the ones that at least fascinate me are these actually computational, if you want, aspects of it.

Ibaraki: I can see DARPA funding your research because they're working on this memory-recording device where you can record your memories and replay it back, and they're doing some early animal studies on that.

Ibaraki: It definitely has to do with memory, and memory compression would be of interest.

Micali: Right. But very, very, very challenging. But again, very future. I answered honestly, but always say I will not know where to start and there other people who are already exploring this before me anyway.

Ibaraki: Now since you mentioned recording, I'm going to introduce another idea. It's about an idea you have, because very early on you had this solipsis about reality versus not-reality. What are your views about the universe and the brain? Do you think the universe has all these millions of brains in it or do you think the universe is a creation of the brain that's contained…? I mean, do you have some ideas on that?

Micali: Well, I have some myths about it, and myths are more powerful than ideas, right? So my myth, which therefore allows me not to explain exactly how, is really that… I mean the brain, the universe, and the divine coincide at the end. So I really believe that. Or put it this way in a more semi-mathematical fashion – I really believe there is a lot of computation going on in the world. Why? Because computation is a human-produced artifact. It's a superimposition of our mind on reality. But at the end of the day, the only reality we know is the one that we experience through our brain. So I do believe that computation should play a role in the law of nature. And if it hasn't so far played a role, then we have the wrong model of nature, okay? That's my myth. And that's it.

Ibaraki: I see. So maybe even in extension, the universe is digital, right? Or…?

Micali: We've… At some point… It's like (a) if it was really me having this conversation, it's a different story. But I'm saying if it is not me and there is, and we are in time with our different entities, I do believe that computation must play a role. Somehow if you look at our laws, so we have no computational not even laws… we use them in computer science, but to describe nature. Sometimes though, yes, we have a program to compute the result, but the law doesn't talk about computation. I think if the law doesn't talk about computation, because it's pervasive in my opinion in what goes on in our brain and ourselves, then we have to rethink our laws if needed to be. Don't ask me how. So that's a myth that I have and I'm sharing my mythology.

Ibaraki: Well, thank you for…

Ibaraki: …sharing some of your mythology, because it will get people thinking. And you're inspirational, so…

Now I'd like to talk about what are some of the most difficult challenges in your research and then some lessons you've learned from these challenges in your research?

Micali: So my challenges are really clear to me. One is my inability to work alone, and two is my limited knowledge. Because I'd love to acquire knowledge on a programmatic basis, but I usually get distracted in solving a specific problem instead and forget about going about laying the foundation of a systematic body of knowledge. So inability to work alone and limited amount of knowledge.

However, I really also believe that… I know for me, like for anybody else, that somehow our limitations are our strength. Let me say… Okay. So I cannot work alone. You cannot work alone? Collaborate. So you have poor knowledge? Be creative, forge your own tools, so you can compensate for it. Essentially it's a really… So limitations are our strength because very often if you're limited, you're going to think of solving a problem in a more interesting angle that those fortunate people who are not limited, that they got to the solution probably in a straight line. In your meandering, you're going to find something else even more interesting than the original target.

And in fact, actually it's so powerful to really realize that limitations are actually strengths that it's actually a good strategy to artificial limit yourself to become stronger. The best example of it is in my opinion is Hernán Cortés in 1519 I believe, that he landed a few hundred people in Mexico in an empire which… I must say he was pretty limited: few people, uncharted territory, much more powerful enemy. What did he do to make him stronger? He made himself more limited. He sank all the ships he came from. It's a famous act, right? So eradicating completely any possibility of retreat. At that point, either you lose or you win. And he won himself an empire.

So I really believe that actually our limitations are our strengths. And if there's advice to give to young people, I'd say, "Be proud and embrace your limitations and make them into your own strength."

Ibaraki: So many interesting ideas in there. Embracing your limitation, but in a way where you're flexible in your thinking as well I think.

Micali: I mean flexibility should be taken for granted. Part of the ability to declare victory is that you can redraw the target whenever you want. Very often somebody thinks that maybe it's cheating because the target ought to be the original target. If the second target is much more interesting, the first one doesn't matter. So I believe actually in fact what is really the right target is really what is most beautiful. I think that aesthetics is a very good guide for figuring out what is right. So in some sense, the right theorem – let's put it this way – is the one who has the right proof. With a few exceptions. But that's what I really believe. I really believe that at the end, you draw a different target. You go to the target and look at it. If it's more beautiful than the other target, that should have been the target in the first place.

Ibaraki: Some really interesting ideas there and I think quite valuable for people. Now you're in a really interesting area and you're amongst theorists. There's got to be controversy. Can you talk about some of the controversy in your research?

Micali: Well, let me tell you some of the controversies. I'm right now involved, and my prediction is that I will continue to be involved, and my prediction is that everybody else will always be involved. And that is somehow the definition of a research area. That is the most controversial thing. Never mind about an approach to solve a problem. That is less controversial than anything else. The first piece of controversy, the most acrimonious where actually friendships are lost if necessary is really defining the area. Because I really think of it… Somehow if you think about theoretical computer science, it's a wonderful scientific community. It's an immensely powerful scientific community. We've done as a community a tremendous number of things, in some sense, speaking of Cortés, as some kind of like modern-day *conquistadores* that are actually trying to appropriate or contribute to different – "contribute" is better than "appropriate" – to different chunks of science. So we have been amazingly flexible.

But yet right now in our conferences, in our journals, what we try to do is that very often you get rejection that say, "This is not theoretical computer science." How can that be? How can it be that we are transformed from the people who wanted to find new problems to solve into the people who should solve the, properly said, older problems? I find that is very wrong.

I have no magic bullet about it, and I can see the other side too. You need to define a research area to make progress, to define rigor, to… But at the same time, you don't want to incarcerate yourself in solving the problems of yesterday. So you must leave room to do this. And this is a continual source of tension.

So right now for instance I'm involved with a few other friends and colleague to somehow launch another conference which is a bit more open, a theoretical computer science conference that is a bit more open to new types of ideas. Because once you see something which is new, you're going to say, "Well, it's not math, it's not theoretical computer science, it's complexity theory. What is it? Well, whatever it is, it doesn't belong to this conference." This is the wrong answer. Those people I think thrive as long as there is… There ought to be walls… Now I'm paraphrasing Reagan, but I'm saying to be walls, there ought to be also doors that allow you to go on the other side of the wall and into the wall. Because otherwise it's kind of asphytic. It's not going to be… We are going to define around there, we are going to make damage.

But by the way, that is really contentious in our community. People get offended if their papers are rejected. I'm no exception. And what do we do? There is really a big danger out there in defining area and there is a great good by properly defining area. So there is a big tension and tension creates controversy.

Ibaraki: Now that's an interesting perspective because everywhere I go, there's always talk about "interdisciplinary, interdisciplinary," but it seems to me there are sometimes walls to prevent that kind of interaction or different ideas or diverse ideas or even outlier ideas. Or this idea that you're the editor of a prestigious journal and really it's in your best interest to kind of do the status quo, and if you do something that's controversial, that's going to hurt you.

Micali: Right! Right, right. Completely correct. By the way, interdisciplinary work I believe ultimately is the most interesting work, but doesn't mean that you can actually sell it. It may actually be very lonely and peppered with a lot of sad feelings and rejections.

I mean even this very paper on zero-knowledge proof, it was rejected five times. Maybe four. Because… So we applied all tricks on the books to make it accepted. First trick is to change the name so that people will not recognize it was the same paper that somebody else rejected before just in case they… Then we change the abstract. We change everything. Nothing. It was canned every single time. At some point in time, finally got accepted. And you know, it needed to be accepted. In some sense, of course Shafi and I and Rackoff, which were a co-author of this paper, we certainly went around discussing it and presenting these ideas. But there is no such a thing like the imprimatur or the seal of approval that a major conference has accepted, and that really helped these ideas to take over. So that is *very* important that we allow this to happen in an official way.

And as a kind of a social engineering of a field, I do not know how we can somehow ensure this flexibility. But I think it is very important that we strike a good balance there.

Ibaraki: I'm intrigued then. You're going to or you have this new conference, or you're sort of in the midst of planning a new…?

Micali: Now I guess it's I want to say a three-year-old experiment. Still there are some very nice papers which came out, but I believe that it should be improved, should be nurtured, should be… And we argue with each other on what is the right way somehow to publicize it, to convince people to publish here. Because again, very often there is *the* prestigious conference. The thing is "Oh, where would you like to be published?" Well, some people, and we cannot necessarily blame them, that there should be one conference instead, the innovative conference. So it's very, very tricky. I really believe that this aspect of science will always be the most contentious aspect of this wonderful enterprise.

Ibaraki: But it's almost like your community is probably one of the most open-minded in that sense.

Micali: Absolutely. And yet, everything is relative. Even the most open-minded community should be more open-minded. At least according to some.

Ibaraki: That's great. Okay. Now can you describe the types of research being created or updated that will drive our experiences in the future, maybe it's 5 or 10 years, and what this experience will be and look like? Can you sort of paint a picture what it is?

Micali: Absolutely not. Because I really believe that if we can predict 10 years out, I mean the future would be boring. I really like surprises and those ones I cannot predict by definition.

Ibaraki: Silvio, what specific challenges in your education at the University of Rome and then Berkeley were catalysts, two inflection points in your lifetime of contributions? And then how and why did this happen?

Micali: How and why. How much time we have? Well, let me tell you one thing. It was not a linear path. I believe that any scientific journey or any personal journey is a path of self-discovery, and self-discovery is a tortuous path. Mine is no exception. Somehow I turned directions several times. Every time that I turned direction however, (a) there was responsibility for a particular person at the turn that maybe made me tack, and after the tack I really knew myself better. I knew better what I wanted. That is only as good as the next turn, but at least I felt that I was improving in focusing and honing whatever I want.

My personal journey now at the university level starts at University of Rome "La Sapienza" in Italy. Italy has a wonderful academic system. At least it worked for me. It's a system in which you can follow four yearly courses. No semester, trimesters. Just from the fall up to the beginning of the summer. Then you follow how many courses you want and then you give a test. You test whenever you want. So in fact you can follow four courses and then, say a month later at the end, you take one exam, maybe another month later take another exam. Then you have the summer to mull it over and before the courses start in September, you take another exam, and so forth. You test whenever you feel ready. For me, that was great because I get sidetracked with things that I like, to the detriment of other things. If I should be tested on all at the end of a year on anything, at least I pass on one and I fail in three. So that system allowed me to survive and I'm very grateful. And it's a very high road system, so you are entrusted to figure out what is best for you and you're treated as an adult and that's the work.

As I was telling you, I started in physics from a classical high school. But never mind, that was not a problem because they started at the time from scratch in the sense that first there was mathematical courses and then physics courses. In fact actually at the time, really an exception was in physics there was for the first time in Italy a semester. So a semester of geometry and mathematical analysis, then physics and experimental physics.

I started first with mathematical analysis. I must say that somebody who is very impressionable, and knows nothing about mathematics, to meet the splendor of the calculus at that impressionable age starting from scratch, not the calculations but really the definition of this notion of infinity properly handled, for me had phenomenal impact. To compound this, I had the most wonderful professor, Luciano De Vito. He was an extraordinary man. He became actually full professor in Italy at the age of 35, which back then was really an exception. And he had a personal crisis or, if you want, an enlightenment, because at that point he stopped publishing anything and became a dedicated teacher for six months and he was in spiritual retreat in the Alps somewhere for another six months.

So he was some kind of a saint. This guy delivered every day, Monday through Friday, 10 to 12, the courses of mathematical analysis, 12 to 2, then all kinds of complicated exercises that he gave in a special little room of the university. Then the poor man tried to go home on foot and I followed him. He never kicked me away. Really a saint.

But what was remarkable about these De Vito lectures were a bunch of things. One thing is that he had a historic perspective. He told you the theorem and also the mathematician who proved the theorem. He had this glorious way of explaining the contribution of this mathematician that you wanted to become a mathematician so that you'd be put in this list by this man. And so much so, just to give you an idea, so he mentioned Gauss, really the greatest. And he mentioned Gauss, so some of us arrived before the lecture and on the full board, we put a gigantic drawing of Gauss. So De Vito came in, "I saw Gauss on the board," he says, "Ah. So the supreme…" and refused to erase the picture. So all the lecture was conducted in a corner of the board which was left empty. We never did it again, because that lecture wasn't so clear and we didn't have enough room, space. Just to give you an idea. So he had this really historical perspective, which are very rare, because most of the people go directly to the theorem and who cares about who invented it. So that was very inspirational in that way.

The other thing is that this guy really required us to reinvent the material. He only suggested problems. Very hard thing to do. I cannot imagine the level of preparation in which you define nothing but you let the people, the audience define things, to drive a discussion so that somehow the right definition without too much intervention is actually gotten. Then after you define, you have to find the tools for solving the problem. So the techniques, the thing. So the entire coach led us to it from scratch. Really a miracle.

At that point, (a) I'm kind of an obsessive personality, (b) I've not yet taken physics, so at this point I say, "Who cares about physics? I want to become a mathematician. In fact, what I want to do is mathematical analysis." So I had this conversation with De Vito and say, "I really thank you. I love the material. Thank you very much. I really want to become a mathematician and do mathematical analysis." He says, "No." "What do you mean, 'No'?" So knowing it was a kind of old-world fashion thing to do to ask the blessing of the teacher to do this transition, but he denied any permission and any blessing. He said that for ambitious young men… Analysis was for older folks like him. He was 45 at the time. He felt that no way that he would allow me to go to do mathematical analysis. There are much better problems to be solved in physics and I should stick to physics.

Then what I did is actually to convince him otherwise, I solved another problem that he gave. I realized that he cared about this problem so I really worked very hard the second year, now Calculus 2, to only solve that problem. At the end of the day, I gave him the solution to this problem. I knew nothing about the rest of the material, let alone Physics 1 and Physics 2, the whole shebang. But I solved that problem. Now I say, "Dear sir, I think now I need your blessing." So then the guy says, "Well, okay. Perhaps a blessing could be done, but on two conditions" – that I do not do mathematical analysis at all costs, but how focus… He did not use the term, but essentially he described the world of Gödel, the world of Turing. That is to say, "You have to do computational…

You have to do theoretical computer science," if you will. He didn't use the term, but that's what he said. I said, "Thank you very much," and I changed.

Now that's my first change. I changed from physics to mathematics. Because I was loyal enough, I actually followed a course in theoretical computer science, which was a course on lambda calculus offered by Corrado Böhm, and a course on logic – not exactly theoretical computer science, but there was not much theoretical computer science at the time in Italy. Then I followed mathematical analysis. Then because De Vito was no longer there, I stopped following Böhm's course and Jacopini's course on logic and I started doing mathematical analysis.

But Corrado Böhm noticed me. I don't know why now, because maybe only some interaction from… I was in the audience. He caught me in the hallway and says, "You, what's your name?" Then he says, "You are no longer following my course." I say, "That is true." What do I say? So "Really I went here out of curiosity." And I didn't want to say it was out of recommendation of De Vito, but I'm saying, "But I really am in love with mathematical analysis." And he says, "Why?" "What do you mean, 'Why?' " He says, "Do you know what I'm going to talk about? So how can you decide like this and get out so quickly?"

So still we're arguing a little bit. Then he did a very smart thing, at least for me. He says, "Well, whatever you do, think about the following problem," and he gave me a problem. That's it. Now he had me. Because at that point, I want to solve that problem. It was a wonderful interaction and he really became my advisor. And somehow eventually we solved that problem, we published that problem. We published also another thing together. But he was a fully immersed and very dedicated researcher. We talked at his house. All of a sudden, his wife Eva, another wonderful person, his kids, say, "Stay for dinner," and so we continued the discussion at the dinner table. So he was very much loved by his family, but he was intense in doing research.

At the end, so I'm now doing lambda calculus and discrete mathematics. First time. I only did continuous mathematics before. This was my first exposure. He told me, "But you need to learn some more theoretical computer science." Okay. So I go to a summer school. It was in Lecce. It was for a month, full-intensive. It was database, other things. Wonderful professors. But one of them was extraordinary. It was Shimon Even. Shimon Even had written a book on graph algorithms and he wanted to polish the book by giving a lecture, and he gave it. The result is that I changed from lambda calculus to algorithms, from logic to algorithms – that's what I want to do at this point – and I follow nothing of the other courses. It's another problem.

At the end, he convinced me also, "You have to go to the States." Somehow Berkeley was the suggested university. I think it was a wonderful idea. I was naïve enough I didn't know that, I only applied to Berkeley, I was lucky that I got in. Then I moved to Berkeley. Berkeley was an indescribable experience. I mean Berkeley at the time, theoretical computer science was getting and must have been a century before to mathematics. So we had Manuel Blum, Dick Karp, Andy Yao. You name it. It was really a place to be. And of course I was absolutely in awe of the place and terrified by the whole experience.

Moreover, my English was so poor. My father, usually my father says, "You have to learn English," because at school, we were taught French. So he says, "Ah, English is the language of the future. Science, engineering, English." He got it right. But for me, somehow I didn't. I don't know. So he sent me to private school in English and I learned whatever I could, but it wasn't much, because as soon as I arrived in Berkeley, I knew that there was a shuttle to go to the university, I could not communicate where was the shuttle to go to Berkeley. Nobody understood me. It took me seven people. Finally I was pointed in the right direction. So you can imagine how much language I knew.

Then I met also a very totally different educational system in which you are tested on the last day of the course and there are homework, homework, homework, which somebody checks that you're actually learning on the way, in parallel on four course. It wasn't for me. I failed tremendously on everything. So I decided, "Somehow I must find some way to declare victory and go home, pack my bags." It was a mistake.

Chance have it that I meet somebody else before going home. Because my English was so poor, they wanted a TOEFL exam, Test of English as a Foreign Language. I had such an abysmal score that they could not let me in in September. I joined in March and they had trimester courses. So I joined in March. By a bunch of prerequisites, not knowing anything about computer science, I take courses like CS1. You can imagine, right? I am – what? – 24. I have 17-years-old as… So no friendships, not nothing. It was a disaster. Plus this educational system, I come out of the trimester, decided to leave.

I meet David. We strike a friendship and David Lichtenstein says, "Okay, so…" By the way, he decoded my English because I used my hands. How did he figure out? Once he gave me a ride to show the good spots in San Francisco, and he couldn't understand me because, by driving, he could not look at the hands. So he says, "Here is what you need to do. Come back in the fall. Don't be afraid. But you need to find an advisor. The most wonderful advisor on Earth is Manuel Blum." Which at the time, he was the chair of the computer science department. "So good news is that he is the chair. He has graduated Mike Sipser, which was his last student, a while ago. He's going to be needing new students because a year from now he's going to be back on the faculty doing research. Tell him that you want to become his student. Good news is that he is from Caracas." Why was that good news? Because according to David, he says, "He knows Spanish, so he can understand Italian." Okay. So

" '*Es claro*' " he says, " '*È chiaro.*' You see, it's the same thing. Just go and talk to him."

Okay. So I went and made an appointment with Manuel. He was the chair. He says, "Well, to tell you the truth, I'm too engrossed in this business of doing the department, of running the department. I don't know what I want to do. I don't want to say yes now anyway. So next… In a year, a year from now is another story," and so on, so forth. So I reported back to David, say, "Thank you for trying, but he's not taking any students." "That's because you have not solved a problem he wants to see solved." So all we had to do is to solve a problem.

So Mike Sipser, a renowned complexity theorist – we just overlapped a little bit at Berkeley and now he's the Dean of Science at MIT – had graduated with Manuel with a thesis in automata theory and left open one question. He says, "How about you work on this question?" I said, "But I don't know automata theory." "Easy." So he invited, "Let's go to a coffee shop. Say you pay for the drinks and I give you lectures." Okay. We sit down and I think four cappuccinos later, he had given some basic definition, he'd given me some little tests, and then finally he was able to enunciate 2:42:41 the problem. Then he says, "Good luck."

So I come back after a few days, I solve the problem. I told David. He says, "Wonderful. Now you go and tell Manuel." So I ask a second appointment with Manuel and I say, "Manuel…" It's actually "Professor Blum." At that point it was. It became "Manuel" because he's a very kind man, but at that point it was "Professor Blum." I say, "I found a solution to this problem." And Manuel, he raised the board, asked me to put the solution on the thing, and at the end agreed to take me as a student, but he still wasn't teaching courses for the next year. But at least he agreed to advise me.

So now I come back to Berkeley and now I'm in the fall and I take lectures on algorithm by Dick Karp. Fabulous teacher. Clarity personified. The timing of the concepts introduced, totally different style than De Vito that I've seen so far, but equally effective. Fortunately, or unfortunately for me, at very few beginning of lectures, he mentioned an algorithmic problem, which is to solve a matching problem in general graphs. So we explain a solution for a special type of graphs, which is called bipartite graphs. It's how to do it in general.

The problem can be described like the problem that a teacher has during a school trip. Assume you have a bus and you have a bunch of kids. Now in every single bus, there are two, two, two, seats of two, right? So as a teacher, what you want to do is that two compatible kids who are friends sit together, because if they're not friends, they are trouble, and then you want to minimize the couples that are mismatched, that are not friends. Not everybody's friends with everybody, so you need to figure out what is the maximum number of seats that you can have occupied by friends?

Turns out that that is actually computationally not a trivial problem. If you try all combinations, it's too much. So he mentioned that problem. Then in the course with me, I had a wonderful colleague, Vijay Vazirani, who became a great algorithmist. So we decide, "We'll solve the problem." We actually did, but I didn't do anything else. In the course, Dick Karp gave me a B-plus, because being the honest man he is, I solved none of the exercises, done none of the homework. All I had to show is this algorithm. This algorithm by the way continues to be for general graphs, as I understand it, the fastest algorithm for matching in general graphs. So he was very, very happy and very proud, but I had a B-plus. And on top of it, I didn't do anything in the other courses. So Dick and Manuel had to intervene to convince the committees, the powers to be that I was allowed to continue at Berkeley. So I'm very glad that they did and I'm very glad they had the flexible rules that allowed me to continue.

At that point, then Manuel is back on teaching, he's no longer chair of the department and he teaches this course on computational number theory which I followed with Shafi, which we talked about ago. But let me tell you that Manuel is an extraordinary teacher in his own style. First of all, his way to convey meaning is by empathy. It's another strategy that I try to copycat best I can. He works wonders.

He works like this. You first think very, very cogently, "What do you want to put on the board in what sequence?" and then you start an argument, then you stop because you lose the thread. And then people don't react, because nobody wants to appear, otherwise you're asked the question if you intervene, so I had to be cautious when to intervene. But when if you're really convinced the professor is lost, and he really look in anguish, then everybody starts, "Hey, you could do this," and then you say, "It's okay. We can do this," and when you get stuck, "Oh, you could do that! Could do that!" At the end, we saw that Manuel really understood the problem.

He was remarkable in another way. He was very slow. That sounds bad, because there was plenty of kids in the classroom which were very quick in reasoning. He's very slow. But he's like a tank. Manuel would work on a problem. It's like a tank moves. "Rrrr!" and then finds a wall. Like the other way, somebody that's very quick, he goes around the wall. He continues, "Rrrr!" full up into the wall and he continues. At the end, it's the "hare and the turtle" thing and the turtle wins. And what a turtle! He has a great mind, has great insight. He goes straight to the problem. Watching that work on a problem is like… I don't know. I don't know the right animal, but maybe a boa constrictor. Or even better a python swallowing whatever a python swallows. Say a wild pig, okay? Slowly, but inexorably, right?

So his way, his technique of solving a problem is really I would call it identification, because it means that the problem is not something that sits outside you. Now the problem *is* you. You became the problem, or the problem became you. And if the problem becomes you, you're going to solve the problem in this life or the next. That's how he solved a problem. You really totally metabolize them and then things, at least for him, became easy. It was a great inspiration for him to see at work.

At the end, so from physics to math for a person, from math to theoretical computer science for a person, from lambda calculus to algorithm for another person, from algorithm to cryptography at that point. Thanks to Manuel every time there was somehow attack… And you know this, if I had to describe the how and why, I cannot be silent about my travelling companions. I mean Shafi of course whom I mentioned, Vijay whom I mentioned, and Mike Luby, the inventor of the Tornado codes, Mike Sipser I mentioned. These were kind of a co-conspirators, kind of a band of brothers who really gave each other tremendous support and really a chamber of resonance or whatever we do. And when we see other people doing things meaningfully and believing it, making progress and sharing with you, and we were poor but happy, it was a phenomenal thing.

To tell you the truth, I would not know it would have happened if I didn't have not only the professor I had but actually the fellow classmates that I had. It was really an extraordinary group and really made me understand that really science is a collective enterprise. Not only it takes a village, it takes more than a village. It takes a scientific community – and that is an international thing – effort and good faith. And in some sense we talk about the Turing Award. Awards are perhaps necessarily given to individuals, but it really is the field. It's the field that matters. It's this extremely powerful social construct.

So I really believe… So that was the best I can say why. I think that everybody else is going to do the same and I think that if there is any message here, it's that it's okay to change. It doesn't matter what, to be totally in doubt, I tormented myself for what I wanted to do, because you can always change. And you should change and you will change and you'll be better off by changing. And you become better at what you do because now you understand what you want to do better and better. It is a great process I think.

Ibaraki: Now I think you also mentioned Andy earlier.

Micali: Yes.

Ibaraki: Can you talk more about his influence at Berkeley and then later at MIT?

Micali: Well, first of all, believe it or not, with my… Actually now you believe it because now I tell you and you have seen what my style is – to go on the problem and don't do the rest. So I never took a course from Andy. However, I listened to a lecture that he did, a lecture that he did on secret sharing. That was

I had just arrived and I made myself a point that I had to go and listen to the various professors, try to get to learn who does what. And to my amazement, not only I understood what he said but I also found beautiful the idea. He was actually lecturing on Adi Shamir's secret sharing. So there you got a lot of things that are admirable about that. First of all, the idea of Shamir that I'm going to tell you in a second, and second of all, that somebody that's finding this idea beautiful, he decides to give a seminar on somebody else's work, because he thinks it's beautiful enough that people should know it too. I'll say it should be the norm. Let me tell you it isn't, okay?

And that actually was in some sense also cryptographic, even though there was no complexity involved, because the idea is that you want to share a secret so that nobody knows what the secret is, but if enough people get together with the pieces that they have, they can now reconstruct the secret. It was a beautiful idea and it actually played a very pivotal role in what I did.

We discussed a lot of things with Andy. In particular, we discussed pseudorandom number generators. I actually had a way to have pseudorandom number generators which were unpredictable, and Andy was actually way better than me in backing up and figure out, "Forget unpredictability. What you want is to pass all statistical tests." And when, if I mention, I'm saying once in a while I missed the ability to back up. That was what at the time I missed. And it wasn't easy, because backing up and thinking that you are done, "What else is there to see?" is not easy. So he was able to see that you had to back up again and having a much more robust notion of and much more of a pseudorandom number generation. That I promised myself was never going to happen to me again. So thank you, Andy, for showing me the power of generalization and not be content with whatever statement of a thing that I have.

Then there are other things. He had a wonderful protocol for secure two-party protocols that I listened to. I was glad to be in the audience because that protocol was never actually published, the details of that protocol. Somehow by having the good luck to be at the right time and the right opportunity allowed me to get this material that then I was able to generalize myself and utilize it later with Oded and Avi, Oded Goldreich and Avi Wigderson.

So he had a very big influence on my life too. Also, he was a physicist for his PhD and became as a physicist to be enamored with theoretical computer science problems. Now he's at Tsinghua. He's directing the theoretical computer science institute at Tsinghua. And we are going to celebrate his 70 birthday. I look forward this December to participate. I mean, so he's a really big impact in my life.

Ibaraki: Now we've been talking about Andy, but for the purpose of the archive, his full name and…

Micali: Ah. Andrew Chi-Chih Yao. Yeah, he's a Turing Award winner. I must say Manuel is a Turing Award winner. Dick Karp is a Turing Award winner. So you can imagine what Berkeley was when I arrived. At the time, neither of them had the Turing Award, but that didn't stop anybody to realize the magnitude of whatever was going on at Berkeley at the time.

Ibaraki: You've had this journey where you've been given the ability to show your talent by solving problems, by being challenged, by taking paths that a lot of people don't take. How does that impact your interaction with your students, with your undergrads and your graduate students?

Micali: I must say I try to be flexible. One thing that actually I realize is that I do not have any rules and I say, "You can work on anything you want. I'm here to help you learn anything you want." I actually try to interact as much as I can with my students. What can I say? I do the best thing I can in terms to pass on the help that I got. I even try, as I said, to copy Manuel somehow. Maybe a bit more pedestrianly than… So if I'm not good at faking that I'm getting lost, at least I can pretend I have a backache to generate empathy, and therefore enhancing understanding. Whatever it is. I try to get it back, and in some ways I have my own style too and I try to push. But I try to… I've already assimilated a lot. In some sense, in my style there is embedded always other styles as well. At least I try to embed them as well, even though I may not do it justice. They were the masters of one particular style and I do my best in my own.

Ibaraki: You have these students coming in and they're like *tabula rasa*, sort of blank slates in essence, especially when they're going into MIT, and they have no idea where they're going to be. Is there any way that you can create a plan for them or help them in their plan, a roadmap or something of that sort?

Micali: Well, first of all I'm also a general advisor. There are two types of advisor. The one, the PhD advisors, in which you follow one student's research and you try to help him or her best you can. That is one type of advising. The other one is that somebody who should sign essentially the card for the courses they're going to take, making sure that they follow all the rules and regulation, and they make, you know, somehow… and you can suggest some questions, some choices or things like this.

So what I've adopted, also because I didn't have a very clean plan myself, is to have this technique. Let's say somebody comes in fresh, for the first time, and so I'm the advisor. I have a questionnaire that I find it easy to have them fill it out before they see me, and they interact with my secretary Linda Lynch. I demand that they write down which course they're going to take when, the grade they're going to take, the people in their committee, PhD committee, in their master's thesis committee, and so on, so forth. And there is an explosion of rebellion that fortunately Linda shields me from. "Huh! How the hell should

I do this?" I say, "If it's not fully completed, Linda, don't let them come to see me. Okay? The end." Because then, I can tell you that it's very hard to say, "You are able to guess. Make up a title for your thesis, master thesis. Make a different title or the same title part two for your PhD thesis. Make up everything!" So somehow, because somehow one misses actually a little bit about "What is the grand plan?" and you go semester by semester and you don't do, and I really want to make sure that people do.

And another thing very often is those who want to go in academia need a letter of recommendation. Believe it or not, you need three letters' representation. And the kids very often, they have only one letter, the one of the advisor, because they've neglected to interact with a lot of people. They don't think duty. So you put there "Who's going to write your letter of recommendation?" suddenly to say, "Oh, gee. So who is…?" So when it starts year two, year three, they start interacting with people, "Who should write the letter?" always they write a very generic letter. "They took my course. They got an A-plus." Good luck. That's not enough.

Then… And people are… But students are wonderful. They're really the reason for which this is the best job on Earth, at least if you ask me. Then they are really unique individuals and I must say I learn from them at least as much as they learn from me. In fact, they learn from each other way more than they can learn not only from me but all professors, all truth be told. As long as we don't try to be on their way, the students are going to do fine.

Just to give you another episode, she was a former student of mine, Jing Chen, and she came from China. A very strong background. And she wanted to do cryptography. It turns out that already I moved on. I wanted to do mechanism design at the time, of which I knew nothing. But somehow I thought it was another way of studying interaction. I really wanted to study that interaction. But she doesn't know and Ron Rivest is on a sabbatical, Shafi Goldwasser is on a sabbatical in a way. I'm the only one and she comes and says, "I want to work with you on cryptography."

First of all, I say, "Thank you very much for all the compliments and things." However, I say, "Why not? Let me actually take the easy way out." So "Okay. Your first assignment is to read this impenetrable paper of mine that I myself cannot read after a few years I've written it," and I say, "Read this paper and come to see me." I say, "This woman is going to disappear. I'm never going to see her again. I solve the problem." So she comes back, it's one week later, and she has really annotated on the margins way more than I've written in print in the thing and says, "You know what? I think there is an error." So on this point, I said, "Oh my God. This is okay. We better read." All of a sudden, I say, "What the hell was I meaning here? I have to understand what I have done myself," which with my memory is really to start from scratch. Fortunate at the end it was very a subtle definitional issue, but at that point I realized this woman is very talented, because that was very hidden stuff.

So I said, “Okay. Pardon my thing. Let me confess my malice,” and say, “I apologize for having you to read this paper. The truth is I’m changing fields. I no longer want to work in cryptography. I cannot therefore advise you in cryptography because I’m working…” You know, “What are you working on?” “On mechanism design.” She says, “What is this?” “Oh,” I say, “this and this and this,” whatever I told you. But she says, “Well…” says, “Alright. How about we work together on mechanism design?” “No, no, no. So I have a position of responsibility here. I know nothing about the subject. I cannot in good conscience accept you as a student in a subject which I know nothing about.” And she goes, “Well, then how about we learn it together?” So then I had to say, “Okay, you are on.” Then we started reading together and then so…

So really no, it’s a great… students are great, and this is a great job.

Ibaraki: Silvio, we’re going to explore some other areas of your background. You co-founded the Information and Security Group. Can you tell me more about that, maybe some of your objective both long and short-term?

Micali: Oh, it’s very simple. It’s to foster interest, education, and research in cryptography. That’s it. It’s a very clean agenda.

Ibaraki: And I guess it speaks to just all of the passions you have. One of the things I want to mention is we’ve been doing this interview now for hours and your energy still sustains. It’s amazing.

Micali: Well, thanks.

Ibaraki: I can see why you have these students that stay with you and probably will follow you forever because of the passion you have, and it comes across. So thank you for infusing us with that passion as well.

Micali: Oh, thank you for your questions. You’re pretty intense.

Ibaraki: Now the next question is about – and I’m going to use the word “passion” again – your passion about the “Advances in Computing Research,” this multi-volume series that you’ve worked on. Tell me more about that.

Micali: Okay. Well, I was the editor. It was the first time that I was an editor of a book. It was a book collecting articles in what was then a very and continues to be a very hot topic, which is the use of randomization in computation. That is this still in some sense mysterious phenomenon, in particular for someone who has never heard about it, that somehow the ability to toss coins translates in the ability of computing what you want faster. So Preparata at the time was kind enough to invite me to put together this volume and I enlisted the collaboration of a very first-class researcher. I was very lucky that they said yes. And so that volume came about.

So in some sense, if you look at a book like this, you have a collection of original research. But also the way I like… not particularly… my book may or may not be good, but exercises like this is that you have on one hand original research, but on the other hand you have actually the coordinate of a journey, where you are and where the community was at a given point in time. Because I believe, in fact actually I lament that not enough time is dedicated to document this. Usually making scientific progress is a very torturous path itself, and what we do is that we linearize it. It is not clear why. Because maybe it becomes more efficient to discuss the material, that's for sure. But in some sense we miss a lot doing so when we erase our tracks and we prevent it from being there.

So why is this? I think that actually it's important to document this. I believe it was Kepler who said that what people know is at least as interesting as how they know it. I totally subscribe to that. I really believe that it's very important to figure out what are the conceptual barriers before the solution. The misconception. Why didn't they see the solution before? And when I say this, I don't necessarily subscribe to the notion that somehow history is a teacher and if you know history, you are likely not to make mistakes. Maybe, but maybe not. But whether it helps or not, I want to know this history. I love stories. Most people love stories. The scientific progress is fabulous stories, and I really want to have this story told and I want to have the story documented. Because useful or not, I like it. And if it is not important to know how we got here, then it is not clear how important it is where we go from here. I think if one is important, the other one is important too.

Ibaraki: Well, that's an interesting insight. I guess this idea that you're not really a subscriber to this notion that "Those who forget the past are doomed to repeat it." You're not about that. It's more about…

Micali: I love the process. I love the journey. Even for its own sake, I find an intrinsic value in the path that was actually taken, particularly if we understand what was going on at that time. I mean we humans are tremendously interesting creatures, but somehow we find that we have to portray our persona after decorating and painting over all kinds of imperfection. I think the imperfections are actually way more interesting than the rest. So how we did these twist and turns, why didn't we get to something, we conceive something else sooner, and what was going on? And that is the type of work that to try to do it afterwards is essentially impossible. Essentially impossible.

Ibaraki: It reminds of Jung where he said something like "Knowledge rests not only upon truth alone but also upon error."

Micali: Ah. Excellent.

Ibaraki: Let's go to our next question here. There are just so many qualities you have, and those qualities have led to enormous success. They've inspired thousands, millions of people out there, and especially your students, definitely have inspired them so that they maybe even become friends because of the qualities that you bring to life and to your work and to the students. How would you quantify that? What are the specific qualities you think that make you who you are, that make you excel, and why?

Micali: Alright. If… It's a difficult question. It's not any easier than the other ones. However, should I try to… The way I feel it is one would be the ability to turn emotions into science. One, I'm afraid to say, creativity. Third would be an admiration of the past. A willingness to gamble the present here and aim for the future. And that's it.

Ibaraki: Those are really interesting ideas in terms of the qualities that make you excel. How do you tie in this idea of emotion? Emotion has given you sort of the energy for power?

Micali: Yeah, yeah. Emotion is really the source of all energies. It's really something that I do not know if we have… It's our ultimate also of inspiration. At least if you believe that there is a common shared humanity, there is some very deep emotional knot that you want to solve. Most probably that is going to found useful also by others and most probably there is something there that we should collectively try to solve. And if one of us solves it, it solves the others as well, or at least it makes a contribution to a better understanding, a better thing. I think scientists or artists, doesn't matter, that is what drives us.

Ibaraki: You talk about admiring the past, and we talked about that in prior questions. And I guess this idea of gambling in the present is being able to take risk, have novel ideas, outlier ideas. And even tying into this conference, this new conference where it's very interdisciplinary, seeking other people's way of thinking and not being sort of locked stuck-in-the-hole thinking. Then yearning for the future. I guess you're always doing that.

Micali: We all should. That's a common shared interest.

Ibaraki: Okay. Past, present, and future then, can you name three or more who inspire you and why is this so?

Micali: Alright. First of all, let me try to make sure that I will not rename anybody who I've already mentioned, because… So I would start necessarily so, and I think I should be in great company, with Archimedes, Newton, and Galileo I think. Just for a very holistic approach to science, they are really my heroes.

A bit more recently but not so recently, I would say Hilbert and Einstein. Never mind they were great minds, but I really admire them also for their romanticism in being a scientist with really a heart.

Then I very much admire our founder Alan Turing for his uncanny ability to solve a problem by conceptualization in which somehow you really understand the problem so well and well and well that at the very end, by magic the solution should sound trivial if you really solve it in the Alan Turing fashion.

And a bit my contemporaries whom I mention and that I really admire a lot is Michael Rabin for his perpetual quest of what is relevant that should really drive all scientists. And amongst my actually schoolmates if you will, Charlie Rackoff, Oded Goldreich, and Avi Wigderson, who are amazing thinkers who really shaped my way of understanding the field by arguing with me vehemently and constantly about what the field is about, what matters, what should not matter kind of. They have contributed way more than whatever papers we wrote together in enhancing my understanding of computer science or science at large.

Ibaraki: We're getting close to some of the questions we're going to ask here. This is pretty freeform. Now you choose the topic area. What do you see as some of the top challenges facing us today? And do you even have any solutions you could propose?

Micali: Well, so I'm afraid that I'm a bit repeating myself because the brain is really in my opinion the one that is really a challenge, and a related one is really education. In a time of hyperspecialization, I believe that this prevents us for solving some very, very, very big problems like the brain. So we must find better ways somehow to have this material penetrate the curriculum even farther and farther back so that we have a very intuitive notion of, in this case, biology, neurobiology, computation, so that we are able to solve this problem. Of course to solve a problem like the brain or anything else, all you need is one person with the right makeup and that's it, problem solved. But if you want to generalize this and if you really want to accelerate the process, if you want to have more chance of succeeding, then you need to recruit more people and to have more synergy, and I think that education is and will always be a challenge.

Ibaraki: I remember hearing that even beyond the planet, you have this idea of maybe we shouldn't be trapped on this planet or maybe we should look beyond this planet. Do you want to explore that at all?

Micali: Ah, yes. That is a total… I think it is a necessity. I think that we should be able to leave the planet sooner than later. I believe that somehow we are trapped on the surface of a very small sphere, and the sphere looked bigger before than it does now. I feel that we are not equipped as humanity to live in so confined a space. And I think it would be very detrimental to our collective psyche if we are not able to do it. One can actually say, "Sure, but there is all other kinds of other infinity of thoughts or whatever that you can do." Yes, maybe. But somehow if you take… even right now you look how many times we use the word "journey," the physicality of a journey is in our genes and when there's no infinite journey, physical journeys that we can do, I'm not sure we can survive this. So we should really for our own sanity to be able to leave the planet as soon as we can.

Ibaraki: We're tying together this idea of the brain, education, and leaving the planet. Do you see some connection with artificial intelligence in this way, a new kind of species happening, and the sort of combination of these three?

Micali: Well, artificial intelligence is a fabulous field. I wish I knew more about it. I'm sure that it is happening right now. Machine learning is a fantastic aid to humanity's decision making. I think it's actually going to enhance ourselves and we create always new tools, and these new tools pretty soon becomes ourselves. It's very hard to separate who is who. I think that we'll benefit from embedding it into ourselves, particularly me with my memory. If I would have some other outside way to help me out, I'll be very thankful. And of course there is risks and fear in everything, so I know that a lot of people could actually fear this change of humanity if you want, if you really embed these things into us sooner than later. But I think there is much more to fear maybe if we don't do it. Then we are really stuck. So our only path is forward.

Ibaraki: I could see that aligning with all of your philosophies and the things that we talked about so far. We're going to ask one more question. You've had an amazing, long, and distinguished career of many, many successes. As a result, you must have some lessons, some other lessons you want to share with the audience.

Micali: Well, I think that the power is the coexisting of opposites, that our emotions are our ultimate powers, and good luck.

Ibaraki: Oh, I just love that. So Silvio, thank you for coming in today. We talked about your family background, your early life, and then we discussed your Turing Award and research, and we followed that by your educational journey and we examined some broader questions. You shared so much and I want to thank you for taking the time to share via this Turing Award Winners project so many of your experiences. I know it's going to be valuable for generations in hundreds of years to come.

Micali: Thank you very much, Stephen. It's been a pleasure and you ask tremendous questions. Thanks.