A. M. Turing Award Oral History Interview with Shafi Goldwasser

by Alon Rosen

Weizmann Institute, Rehovat, Israel

November 23, 2017

Prof. Rosen: Hi. My name is Alon Rosen. I am a professor of computer science at the Herzliya Interdisciplinary Center in Israel. Today is the 23rd of November 2017 and I'm here in Rehovot at the Weizmann Institute of Science together with Shafi Goldwasser, who is being interviewed as part of the ACM Turing Award Winners project.

Hi, Shafi. We are here to conduct an interview about your life, about your achievements. We will go chronologically according … generally speaking chronologically and we will talk at two levels. The first level will be a general audience type of level and the second level will be more specific, more oriented towards people that specialize in the subject and are interested in the details. Let's begin. So could you give us some family background? I'd be interested in your parents, where they came from, what they did, and maybe your earliest memories.

Prof. Goldwasser: Okay. Well, first of all, thank you Alon for taking this opportunity to interview me.

My family background? I was born in New York actually, in Sea Gate, which is right outside New York City. It's sort of a beach community. We were a family of four. I have an older brother who's six years older than me and my parents were Israelis who were actually visiting the United States for a period of time. My father was representing the Israel "Kupat Cholim" (קופת חולים), which is the health services at the time. He was recruiting doctors, recruiting donations, buying equipment for the Israeli medical service we were just starting.

And my earliest memories? That's a good question. I think I remember something about going to the beach in Sea Gate, you know, which is where we lived. Because my mother used to take us to the beach every day, and I remember there was a lot of wind on the beach. And I remember sort of one of my balloons, or maybe it was a floatie of some sort, sort of flying away. But it's not very relevant to my career going forward, [laughs] except I've always liked the beach and that might be related. And my mother was a homemaker.

The background of my family is that my father was born in Poland before the war. When the war broke out, World War II, he was a student, a law student in Krakow. But as the war broke out, he came back home to where his family, which

was in Bielsko, is a town in Poland, not far from Auschwitz actually, in between … And he, with some other young Jewish men, which were around I think 19 or something like that, 19 years old, they escaped to Russia. And from one thing to the other. He was in Russia, he was in Siberia. Somehow he joined these units of the Polish army that joined the allies to fight the Germans, and through a very roundabout way at some point they landed in Israel and he stayed in Israel.

When he stayed in Israel, he was without anything. His family was … He had no idea where they were. He thought they all perished, but it turned out they didn't all. Some of them did, but his mother and his sister actually survived the war. You know, they were in camps, but later in some … He thought his mother was dead, but after the war he got a letter … He wrote a letter to a neighbor and the neighbor said that his mother is living next door. So he went back around 1947 or 1948 and he eventually brought her back to Israel.

But he met my mother during those years, and my mother's a completely different story. Her parents came to Israel in the '30s and they were some of the people who founded a town in Israel or a farming community called "Kfar Vitkin" (כפר ויתקין), and she was born in Israel. And they met because he rented a room in their house and she was giving him Hebrew lessons. So she was away actually in school and she would come back on vacations and she was giving Hebrew lessons. She always told a story that all of a sudden this very strange man from Poland who didn't know Hebrew and had very kind of polite mannerisms asked her, "Would you marry me?" and she was like, "No." Like, [laughs] "Who are you?" But apparently he was very charming.

But in any case, those are my parents. I also have a younger sister. She was born years later after we came back to Israel.

Prof. Rosen: And did you come back … where did you come back to in Israel?

Prof. Goldwasser: We came back to Israel when I was six. We came back to Tel Aviv. So we came back straight from New York to Tel Aviv.

Prof. Rosen: And where did you live in Tel Aviv specifically?

Prof. Goldwasser: In Tel Aviv, I lived … it's near a place called "Kikar Hamedina"(ככר המדינה) . It at the time was considered sort of the north part of Israel. I think now it's called the Old North.

Prof. Rosen: Of Tel Aviv?

Prof. Goldwasser: Of Tel Aviv. Not of Israel, of Tel Aviv. Yeah.

Prof. Rosen: I have a question actually about your father's childhood. I heard a story that he was studied with the Pope or something, with John Paul?

Prof. Goldwasser: Yes, that's right. Bielsko is actually part of two towns. It's called Bielsko-Biała. And there's a sort of river that runs between Bielsko and Biała, and the Pope was from there. I think that maybe he's from Biała and my father's from Bielsko, and they were in the same high school. And my father always said that he knew the Pope, and this sounded like some of these stories which … [laughs]

Prof. Rosen: We don't believe.

Prof. Goldwasser: Which sound like fantasies. But it actually turns out then I met people who went with my father to high school, and they were actually in Italy because they ended up … after the war they stayed in Italy, and they would see the Pope regularly because they were part of an acquaintances group.

Prof. Rosen: And he got to meet him again, or … ?

Prof. Goldwasser: My father? I don't think so, because he didn't really go back to Poland for many years. No, I don't think so. They were not close friends. They were in the same high school and they knew of each other.

Prof. Rosen: Okay. Let's go back to the thread to Tel Aviv. So you came back to Tel Aviv after kindergarten in the US?

Prof. Goldwasser: Right. So I was in the US till age 6 and I went to kindergarten, to this kindergarten called Bialik School. There was a Bialik School and they had a kindergarten. That's another memory that I remember from New York. There was a kindergarten and the playground was on the roof. You know, like there were slides and a sandbox I think, and I remember you would sleep in the afternoon there. There was a big room with mats on the floor. In any case, we came back to Israel when I was around 5 and a half or 6, and I came to first grade to a school called "A. D. Gordon", which still exists in Tel Aviv.

Prof. Rosen: That's a famous school.

Prof. Goldwasser: It's a famous school, right. It's sort of a proletarian school. I came not exactly mid-year, but a few months into the beginning of the year, and I think that for the rest of my duration of school, which is eight years, and even today they remembered me as the girl who came from America. Which shows to you how Israel was at that time, that that was such a rare occurrence. And because I didn't know Hebrew for the first few weeks, I think they sort of remembered me as someone who didn't know how to speak Hebrew in the beginning.

Prof. Rosen: Do you remember any specific day or any specific event from the return, from …

Prof. Goldwasser: From the return.

Prof. Rosen: … around the time of return? Your first day for instance, but not necessarily.

Prof. Goldwasser: In school? At school?

Prof. Rosen: Yeah. Not necessarily.

Prof. Goldwasser: No. I remember actually some funny event, which is unrelated to the Turing history for sure. But then my parents were renovating this apartment in Tel Aviv, which actually my parents lived through the rest of their lives in and I actually own it now. While they were renovating, I was staying with my grandmother in Kfar Vitkin and I was very attached to my mother. She had to go to Tel Aviv to … I don't know, to supervise the renovation, and she couldn't get away from me so she locked me in the bathroom. That I remember there, yeah. This is not representative. She was actually a very good mother. [laughs]

Prof. Rosen: But it's representative of the era, of the time?

Prof. Goldwasser: Yes.

Prof. Rosen: Okay. We're back to go to the elementary school and then middle school I assume if it was in … ?

Prof. Goldwasser: Well, in Israel, it's like one to eight, yeah.

Prof. Rosen: One to eight. You said it was a proletarian kind of … ?

Prof. Goldwasser: It's sort of … it's a school that was unusual for Israel at the time. I actually don't know really if it's unusual at this point. I think it is. Like, for example, we ate there. You know, there was a lunch and there was a very, very big room with long tables where there were probably 12 or more kids per table. And before we would eat lunch, there would be news that we were being recited and then we would sing some songs and then we would eat. I kind of hated the food, I remember that, especially the oatmeal [laughs] or "daisa" (דייסה)that they would make. And I remember that one day they wanted me to stay and eat everything, because you're supposed to kind of clean your plate, especially at that time I think in Israel. And my mother happened to pass by and she told the teacher that I don't have to eat whatever, there's no need for force me to eat anything. That again, another very strong protective memory of my mother, that I knew that I could really do whatever I want, which was always true.

Prof. Rosen: And, okay, about the atmosphere, I'm curious about the atmosphere in the school and how you related to it.

Prof. Goldwasser: Yeah, the atmosphere at school was very sort of … very Israeli, very rooted in the Israeli culture. [0:10:00] It's a school that I think a lot of sort of famous figures from Israel history went to. You know, Yitzhak Rabin and some other famous people. In fact, it wasn't near home, so I had to take a bus to go to school, which was an unusual thing in Israel. But my parents heard about the school. They asked before they came back, which school should they send Shafi to, and they said this particular school because this is a school for "Tnuat Haavoda" (תנועת העבודה), or whatever, particular political party, the ruling party of the day, and that it's long hours and it's good education and good fundamentals.

In any case, I went to this school. So I took this bus number five every day to school and back, and except in the morning. My parents used to go to the beach every day in Tel Aviv, because my father loved swimming, and so did my mother since she grew up in Kfar Vitkin, which was near the beach. And we used to go every day. Six o'clock in the morning we would take the Dodge Dart, which we brought from New York, and drive to the beach. And I'm mentioning Dodge Dart not because it's such a fantastic car, but at that time in Israel they didn't exist. I remember that … there's another memory that in the United States we had this car, and it was just a small car. Then it arrived on ship to Israel and it was huge, it was like the biggest car ever in the streets. And we had this car for a very long time. We used to go to the beach every day in the morning and then they would take me to school.

Prof. Rosen: And did you feel that you belonged in the atmosphere of the northern Tel Aviv at that period, or were you different?

Prof. Goldwasser: Northern Tel Aviv was very laid back at that period. I don't think it's what people think of today. Yeah. I remember there were these two kids in the building that I used to play with. They didn't go to the same school because the school was far away, so I rarely saw the kids that I went to school with. But the atmosphere was very … it was a much smaller town. It certainly was not the lively Tel Aviv that people think of today. The school, as I said, there was a lot of singing. You know, Sunday morning there was an hour of singing, all kinds of songs. You know, these sort of Russian melodies but Hebrew words. Celebrating all their holidays, a lot of Israeli holidays, as you know. Then in terms of schooling, you know I loved literature. I loved sort of history and stories of the Bible.

Prof. Rosen: Do you remember specifics about which literature …

Prof. Goldwasser: Which literature?

Prof. Rosen: … and which stories in the Bible?

Prof. Goldwasser: From the Bible. I just want to explain the stories in the Bible are not religious stories. In Israel, you learn sort of stories in the Bible sort of from first grade on. And it's always, at least in the school that I went to, it's really stories. So there's a narrative about characters that you get attached to, at least I did. I've always liked to read. Do I remember specific stories?

Prof. Rosen: Which are the kind …

Prof. Goldwasser: Yael and Sisera, I remember that. There's a story of Yael, who was someone who helped the Israelites and she … There was this conqueror or fighter. I don't know exactly the name in English. I would know how to call that in Hebrew. And he was tired, and he came to rest at her tent, and he asked her for water and she gave him milk. And then she killed him. This is all in order to protect the Israelites. Then because she was part of this pacifist tribe, she was then punished by her tribe for this murder, but she was hailed as a big protector of the Jewish people. [laughs]

Prof. Rosen: Interesting parables.

Prof. Goldwasser: She was a strong woman.

Prof. Rosen: Okay. And about what literature?

Prof. Goldwasser: If I remember something specific. Actually, I can't remember right now. But I do remember I wanted to be a writer, and me and a friend, or a friend and I, we decided to write a newspaper. So we organized this little newspaper with stories, and we said we were going to charge kids two cents or two "grush" (גרוש) in Israeli, and I think that we had a third friend that she bought one of the copies. That was it. There was one copy, there was one customer. [laughs] It was a very short-lived experience.

Prof. Rosen: What about friends? Do you have any particular people you remember from the period?

Prof. Goldwasser: Yeah, I remember I had a lot of girlfriends.

Prof. Rosen: Can you mention them?

Prof. Goldwasser: Yeah. There was this girl called Racheli Ben David (רחלי בן דוד). Their father worked in the city hall, and he had an office very … at the top floor in the city hall, which is in Kikar Rabin (ככר רבין) now, and we used to throw things. I used to go there and visit Fridays at the end of school and we used to throw things from the top floor. I mean I don't know, things, like paper planes. Then there was Maya Galperin (מאיה גלפרין). She was another friend that I kept in touch with for many years. So those are the people that I remember. There are a few others.

Prof. Rosen: And are you still in touch with them?

Prof. Goldwasser: I'd lost touch for many years, and then I re-connected with Maya, for example, years later, because she went to high school as well with me. But I didn't keep close friends from that period, from the elementary school.

Prof. Rosen: And can you tell us a bit more about your relationship with your siblings?

Prof. Goldwasser: I have one brother who is six years older than me, Nati (נתי) . Then I have a sister who is eleven years younger than me. I remember when she was born. I was in the sixth grade or something like that. My parents went away for vacation and nine months later she was born. In fact, I remember that I'd made a deal with them. I really wanted a dog, and they said that the dog I won't get. So then I said, "Okay, so either a dog or a sister," and we wrote this contract. And I have it actually. I found it a few years ago, when I was cleaning my parents' apartment. In any case, I got a sister. I have a dog now, not then. Yeah, it was very, you know, we were living in this apartment, which seemed to be plenty big, but in the standards of today it's quite small. And we, again, used to go to the beach and my little sister, I felt very protective of her. I remember taking her to daycare in the mornings and she … When my mother would take her, she wouldn't let my mother go away, but when I took her, I would just put her there and go to school. This is already high school.

Prof. Rosen: Yes. Okay. Anything else that you would like to tell us about from that period?

Prof. Goldwasser: Yeah, I guess so. I mean just one thing is that my grandparents from my mother's side … Because I told you my father had a mother and a sister who went through the war and then arrived in Israel. Some interesting story also somehow, like they brought the son of the sisters illegally into Israel because otherwise the grandmother wasn't willing to come. But my grandparents from the other side, from my mother's side, they lived in Kfar Vitkin, they had an agricultural farm or unit, they had cows and chickens, and I had cousins there. We would spend every weekend, we would go there for spending time with them, having lunch, going to the beach. Sometimes I would spend weeks there in the summer. So this connection with this farming place or "*moshav"* (מושב) is very strong in my mind. That is really childhood, that and the beach.

Prof. Rosen: There's a bit of contrast between the urban Tel Aviv that is bourgeois and the agricultural working part?

Prof. Goldwasser: Right, although I don't think really my upbringing in Tel Aviv could be described as bourgeois. Even though because of the school that I went

to and because of my mother coming from this "*moshav*," she really was not … she was not a bourgeois type. You know, she didn't take care of herself so much. The house was, you know, very casual shall I say? It wasn't a very formal atmosphere and it wasn't a very fancy atmosphere, so it's hard to …

Prof. Rosen: But you didn't feel like an outsider in Tel Aviv, for instance?

Prof. Goldwasser: No, no, no, no.

Prof. Rosen: Okay. So let's move on?

Prof. Goldwasser: Okay.

Prof. Rosen: High school?

Prof. Goldwasser: High school. Right. Then high school, it was already a different story. I went to a high school, it was next door. You know, it was the "Tichon Dalet" (תיכון ד') and so I didn't have to take the bus anymore. All my friends from elementary school, they went to different high schools Hay (ה') because they were from the neighborhood near the elementary school. So it was just me and another girl, Maya, and maybe one other that went to this new school.

Those years I remember quite vividly. The orientation changed a bit for me from sort of being interested in the sort of more humanity subjects to more the mathematical subjects. You know, mathematics, the science. I remember I loved physics. I didn't really like life sciences, but physics and math I liked quite a bit. And I had a great teacher, it's Uri (אורי), from eleventh and twelfth grade. Somehow I did well and I think that was part of why I wanted to do it. And I had another teacher for physics, his name was Zelikovich (זליקוביץ') , and physics in my mind was just fantastic. You know, things made sense, you could derive things. I think early on that's what I wanted to study.

Prof. Rosen: What about mathematics?

Prof. Goldwasser: In mathematics, you know again I was good at it, but mathematics itself at that time was not described as mathematics with sort of motivation. [0:20:00] It was more the method, you know? So taking derivatives, integrals, and it was in trigonometry and all that. And I could perform it well, but it didn't have the stories associated with them that physics did.

Prof. Rosen: So it was more about the technique and less about … ?

Prof. Goldwasser: About technique rather than about motivation.

Prof. Rosen: And did you already then have the sense that you missed the concepts and the … ?

Prof. Goldwasser: I had no idea that there were concepts, you know? All I knew that I liked the concepts in physics. The whole derivation from principles was beautiful in my eyes. And I remember questions on the exam and then you would have to think. And I have the impression of some memory where my [laughs] answer was different than others and he was surprised, the professor. But I cannot, for the life of me, remember what the question was or what the derivation was.

Prof. Rosen: So it sort of sounds like this professor, he had an encouraging influence on you.

Prof. Goldwasser: Yes, both of them. Yes.

Prof. Rosen: Ah, these are two different people?

Prof. Goldwasser: Yes, Uri was a math professor …

Prof. Rosen: Uri

Prof. Goldwasser: … and Zelikovich was this physics professor.

Prof. Rosen: Okay. How significant do you think it is?

Prof. Goldwasser: To have a good professor? To have someone who influences you that early?

Prof. Rosen: Yes.

Prof. Goldwasser: Extremely significant. I think if you're very lucky, there is someone early on – and that could be high school, it could be maybe college, but better in high school – that awakens something in you, that somehow a spark, an interest, so that maybe later you're not going to do exactly that but you know there's something about studying and about pursuing knowledge that is exciting. I think it's fundamental, and I don't think that it has to be more than one. I had other good teachers there, you know. The literature, I remember the teacher. The history teacher. I remember learning Shakespeare in English class. But something about … there was some spark there in the science classes and in the math classes that I recall.

Prof. Rosen: So by then, your self-image was sort of that you were set towards studying scientifically-oriented subject?

Prof. Goldwasser: No, not at all. [laughs] As I said to you, I love to write, and I think that my inner image was that I was going to be a writer. But I guess – you're right – by the time we got to the eleventh and twelfth grade, my parents, or especially my father was very kind of insistent that I should follow the realistic … this is what we call in Hebrew "realistic studies," or mathematics and physics studies. Because as people of his generation, and maybe people of the current generation in Israel as well, there was a real emphasis on pragmatism and the exact sciences, and that everything else is a bit less … it's fun. It might be enjoyable, but it's not as real as what one must do in life. And I …

Prof. Rosen: And what do you think about this Israeli tendency?

Prof. Goldwasser: What do I think about this Israeli tendency? It's a good question, right? On one hand, you can't argue with success. I mean Israel's doing very well. This whole idea of a "startup nation," it's not a phrase, it's the truth. You see the talent that's coming out of here, you see the ideas that come out of here, the technology, how we are able to compete with the rest of the world. I think part of it is this drive to go into science, go into technology, excel at it. So I can't argue with success.

On the other hand, there's a lot of art that has developed here over the years. Art, writings. When I was little, that was not as developed. Even the whole culinary style that exists in Tel Aviv. The whole idea about having a good life, "a good life" meaning that is composed of art and music and film and food, that was not part of how I grew up, in the sense of importance, but it is part of Israel today.

So what do I think about it? I think that it would be better if there was importance, a stated importance on humanities,

[0:24:34 audio drops out for 3 seconds]

… philosophy and art and literature. It exists, but I think that in the scheme of things people seem to have more respect for studying exact sciences. Certainly in high school it was the case. So when my kids were studying in high school here, it was very clear that the kids who were studying math and science are more … better thought of. I think that may change later, but it certainly was the feeling I got watching my kids and their friends.

Prof. Rosen: You seem to have suggested that it's been changing a bit in Israel.

Prof. Goldwasser: No, I'm saying that there's also a whole other subculture that pays attention to film and all these other fields which we've mentioned, which I've mentioned. But it belongs in pockets. You know, I don't think it's infiltrated in everywhere. It's still like when I was growing up, but perhaps not completely. I really can't speak in such authority about Israel because I spent … I left Israel when I was 17 and a half and then I spent most of my life or at least half of my

life in the States. So I would hate to come across as a figure that speaks with authority about what Israel is like today.

Prof. Rosen: Yes, but you do have perspective …

Prof. Goldwasser: I do have perspective.

Prof. Rosen: … and from the distance it's actually beneficial.

Prof. Goldwasser: From inside and outside, it's kind of coming and going.

Prof. Rosen: Yes.

Prof. Goldwasser: I've done a lot of coming and going.

Prof. Rosen: Yes.

Prof. Goldwasser: Yeah.

Prof. Rosen: We'll talk about that later**.**

Prof. Goldwasser: Uh-huh.

Prof. Rosen: Up until now you were talking for the most part about your personal experiences and chain of events. I'd be interested to hear now about your view on the global experience of Israel at the time.

Prof. Goldwasser: Sure. Yeah, I do have the tendency to talk about the personal stuff, but it's what I know best. But let me tell you a little bit about my memories about Israel. First of all, I lived here through a few wars, right? I remember the Six-Days War. I think I was in sixth grade. No, fourth grade. Fourth grade?

Prof. Rosen: Yes.

Prof. Goldwasser: Yes, fourth grade. I remember that. And I remember we went down to the bunker, to the *miklat* (מקלט). I remember the sirens. And I remember right after the war, my family and I, we drove to Jerusalem. I remember still seeing the Wailing Wall before they kind of opened up the big, you know … How do you say it?

Prof. Rosen: Rahava **(רחבה)**

Prof. Goldwasser: Rahava. But how do you say it in English?

Prof. Rosen: The big square.

Prof. Goldwasser: The big square in front of it, there was this kind of a narrow street. I remember going there and seeing it. And I remember actually going to Jerusalem before that and seeing where the border with Jordan was, and there was like Jordanian soldiers. Then that was gone, and there was just the wall and we were walking all around Jerusalem. It was somewhat of a euphoria. Who knew that this would be a … as we say in Hebrew, "Bchia Ledorot" (בכיה לדורות) .

In any case I remember that. Another thing I remember about the war is that there was a friend of mine who lived in the same building. Her name was Karina (קרינה). Her parents sent her when the war broke out, because she had relatives that said that they must send her. And after she came back I was telling her about the war, about sitting in the bunker, about what it was like, and she said, "Ah, it sounds like so great. I wish there was a war right now." [laughs] I remember even as a child it sounded like a funny thing to me.

But in any case, this is fourth grade. Then I remember Yom Kippur War. Yom Kippur War is a different story. Then I'm already in tenth grade I think and my brother was a soldier. I remember it was Yom Kippur, and this was the first Yom Kippur ever that I was going to fast. Me and I think the same Karina, we decided we're going to fast together, and we walked around near the Yarkon (ירקון) , which is sort of a river that runs through Tel Aviv. And when we came back, we saw lots of cars. It was like around one o'clock or something like that, or 12 o'clock. Lots of cars driving, and it's very atypical for Yom Kippur. When I came home, my brother was there, because he was in the army but he came home for Yom Kippur. He told us that there's going to be a war. In fact, maybe the hours are being mixed up a little bit. Maybe he said it earlier. In any case, he said, "There's going to be a war," and my father said to him, "What are you speaking nonsense for?" It was like, you know, because Jews that came I think from the war, another war, the whole idea of talking about death and war was something that you just don't talk about it, because it's just bad luck or you just don't say things like that. Then he was called and then he left, because he had to go back to the army, and then we didn't see him for a few weeks.

Prof. Rosen: Where did he serve?

Prof. Goldwasser: During his military service at that point, he was actually in some sort of [0:30:00] an intelligence unit. But his intelligence unit joined Katyushot (קטיושות) , which are these artilleries, and they kept on going from the north from the Golan Heights to the south to the Sinai, back and forth, back and forth. I remember the first phone call that he called and my father asked him how was his commander, who was someone that my father felt that was going to protect him. And he said, "He's no longer." And I remember my father just burst out crying. He was just so, so, so worried about him.

Prof. Rosen: How did you feel about the … ?

Prof. Goldwasser: You know, I remember in school we were filling … we did these things. We filled sacks of sand, you know, for these trenches. We went to a place where we packed food for soldiers. I think it was for soldiers, or for in the case of some sort of evacuation the people will have these bagged foods. It's a very confused time, right? Especially you're worried about your brother, what's going to happen with him. Then I remember when he came back home the first time … I don't know how long it was really because he stayed in the army for about six months afterwards. He was supposed to be released but he stayed longer because of the war. But I remember that he had a lot less hair. He had like those two sides of his forehead, his hair receded quite a bit. It was amazing that this kind of traumatic experience can do that. So he went with a full head of hair, and it receded.

Prof. Rosen: And at the time, okay, I was asking more how did you feel about your father crying?

Prof. Goldwasser: Oh, about my father crying. It was a little scary. He just kind of lost control, you know? Because he didn't … he wasn't a crying man.

Prof. Rosen: Do you think any of this had any effect on you in the long term, on your personality, outlook?

Prof. Goldwasser: I think it had an effect on my father. I think that when my brother came back from the army, he joined the Hebrew University, because he was going to go and study mathematics, and he went right away. They postponed the semester because of all these soldiers … They started a new semester in January, like a new school year. But my father just wanted him out of Israel as fast as possible. He was so afraid for his safety that he wanted him to go to school in the States. And within a year, like the second year he just sort … he somehow arranged … he kind of made him apply abroad. And he got accepted to Carnegie-Mellon and he left. That affected me because that started some sort of chain reaction in the family.

Prof. Rosen: And okay, you said your brother studied … wanted to study mathematics. What did he end up doing and … ?

Prof. Goldwasser: My brother … He studied mathematics as his first degree, and then he went to business school at Carnegie-Mellon. It's called GSIA, Graduate School of Industrial Administration. And then he went to work. And I, when I arrived at age … I had like a year or so before my military service and my father wanted me to go to the US to study so that I don't waste any time. This idea of wasting time is something very problematic, or was very problematic when I was growing up. Now it seems like everybody's just taking trips around the world as soon as they finished the army, before the army, and wasting time is not called "wasting time" anymore but "gaining life experience." In any case, my

father wanted me to go to the States, and as usual I did what he recommended and went to Carnegie-Mellon, and I went to study mathematics.

Prof. Rosen: I'm curious. You say your father recommended, and so did your mother have any say, any influence about your decisions?

Prof. Goldwasser: I think she agreed with him. I don't think she was … She was dominant in the sense that she … I remember her there all the time. She was extremely … I remember her cooking and I remember her doing homework with me, and she was very much into the humanistic subjects. So I remember reading with her and talking about these biblical stories and history. But in terms of these decisions, I think she just kind of agreed with him or didn't object to him. She also did say to us, both me and my sister throughout growing up, is that a woman has to take care of herself and she has to be independent, it's extremely important. And I think that probably was because she wasn't. My father was the one who was the breadwinner, and I think in her mind, anything that was a step toward accomplishing that was a good step. And I don't think she thought about the fact that that meant that I was going away, or if she did think about it, she thought it was worth it.

Prof. Rosen: Any other anecdotes from the childhood period in Israel relating to your view of the era?

Prof. Goldwasser: Well, you know, my high school … no, not my high school, my elementary school was near Sderot (שדרות) Ben Gurion. Ben-Gurion's house was very close by, and we used to go by there and see the guard. [laughs] So I remember that, that Ben-Gurion was a big figure, was a big looming figure. This whole idea of him being in the house or being in the desert, his whole view of the desert and the importance of populating it.

Then another maybe anecdote that has to do with the Israeli scene at the time, not a personal scene but not to do with the wars, is when – this is the '60s – when the prime minister of Israel at the time Eshkol died. I somehow remember that they told this to us in school and there was such mourning. You know, all the kids burst out crying. Like why would they? I mean, but there was such a feeling that you were a member of a global tribe or a local tribe, and even that infiltrated all the way down to sort of young children who felt connected and felt that they knew who this man was. Now it could be because of the school that I went to, that all of them were kids of families from the Labor Party, what's called Labor Party now. Then I think it was Mapai (מפא"י). And also I grew up in this kind of a home. So these are sort of memories about these figures bigger than life – you know, Ben-Gurion and Eshkol.

And I remember that we read newspapers feverishly, every day. You know, three newspapers from cover to cover. And I had tremendously strong opinions about Israeli politics, what's right and what's wrong. Like one of the discussions I

remember we always had was whether the Jews in Europe were the same as the Jews in Israel. You know, whether they were … we should be ashamed at … There's this Israeli sentence "Ka Zon Latevach" (כצאן לטבח), that they went into these camps as sheep and they didn't resist. This was a big myth in Israel. And I was always very much against it, and I was a very singular voice in my class. I remember we had these debates where a lot of the kids were like, "We're not like them." To me, it was sort of obvious that we are exactly like them and that who can judge people in that situation. You know, after being starved for years. So I remember these kind of political debates with many of them and I had lots of very strong opinions about this.

Then I remember also the first terrorist attack in Ma'alot where there was a school that … it was a school trip and the school was … while the kids were sleeping there, there was a terrorist attack from the north. You know, it was so real, it was so vivid, it was so part of our lives. Like we would know blow by blow. Of course, it was overdone, because they would describe everything in such graphical, yellow-journalistic details. But one must forgive it because it was the first time and I think it was a shock to such a young country that didn't realize what it was doing. And as kids, these are extremely powerful and somewhat traumatic images, to think of other kids and what's happening to them. Then there was the whole debate about teachers, did they stay in the school, didn't they stay in the school, did they protect the children? And again, my view was … You know, there was the judgmental view, which is "You must protect the children because you are the teacher," and then there's the view that they're people and they also have families and kind of impulses that they cannot control of protecting themselves. I think that in that situation my opinion was that they should have stayed. So there was some moralistic [laughs] line in my judgmental opinions about these events.

Prof. Rosen: So you describe it in hindsight with a cynical point of view …

Prof. Goldwasser: Mm-hmm.

Prof. Rosen: … but how was it back then?

Prof. Goldwasser: What do you mean?

Prof. Rosen: How did you perceive all the events? Did you have a cynical outlook already?

Prof. Goldwasser: No, no. Not at all. My father was a big cynic, but not about things like that. But certainly cynicism and humor and seeing things in somewhat of a perspective, which is there's the big picture but there's reality, is something I got from home. But I think at that time, as a kid, I was resistant to that. It was very annoying to me that my father was cynical. And now, as to be expected, I am cynical myself.

Prof. Rosen: And do you feel there was a period where you had a transition from the innocent view of a child to … ?

Prof. Goldwasser: Eh, no. I think it just happens with age, doesn't it?

Prof. Rosen: Age over time?

Prof. Goldwasser: Yeah.

Prof. Rosen: Because you did describe that you had a contrary view to your peers.

Prof. Goldwasser: Yeah. [0:40:00]So I certainly think …

Prof. Rosen: So it's an indication?

Prof. Goldwasser: … that I've always had my opinions and I've always thought about things in my own way. I mean I don't know if it has anything to do with the fact that later on I went on to be sort of a scientist or someone who invented things, but I always remember this thing about crossing the street and how people usually cross the street together, you know, when the lights turn green, and that I would always cross the street either before or after and it always would be surprising to me that people would wait for other people to cross the street.

Prof. Rosen: Do you have any other examp- … anecdotes …

Prof. Goldwasser: Of that sort?

Prof. Rosen: … of that sort?

Prof. Goldwasser: No. I think these political debates is this crossing the street, it's this … I can't think of another episode. But I must say that home was very supportive of this. My father was not a usual man. He did not have typical opinions. I've described him so far as sort of an outcome of his generation, you know, that he was pragmatic, but he had very unusual opinions. The fact that he wanted me to study, he wanted me to go abroad. You know, there was no difference between men and women here, and he thought we could do anything. That was very unusual, and that was true all along. You know, this whole idea that women should behave a certain way, they should get married, they should have families, that was *completely* beside the point for him. And he was very vocal about that. And he thought I was bigger than life. That was a good thing, to grow up having that image of yourself.

Prof. Rosen: So you already grew up with this feeling that …

Prof. Goldwasser: The empowerment.

Prof. Rosen: … you have the capacity and empowerment?

Prof. Goldwasser: Yeah. Life certainly kind of beats it out of you, but certainly as a child that was a very important sense that my parents gave me.

Prof. Rosen: So from both parents? It came from both parents?

Prof. Goldwasser: Well, my mother was just a very loving mother, so she was very … she was there. I think she gave us a lot of love. I mean my father gave this feeling of power.

Prof. Rosen: And in school, how was the … ?

Prof. Goldwasser: You know, I was a good student. I was a good student always. And I felt that the teachers respected me, those who did respect me, so there was no contradiction to that.

Prof. Rosen: So for you personally maybe not, but this talk that women are … society is directing women, driving them away from …

Prof. Goldwasser: Right. There is such talk. I certainly didn't feel in elementary school. In fact, nobody says that's true about elementary school. They usually say that starts in high school. In high school, I had one math professor in … early, fifth grade or sixth … fifth, that's ninth grade, ninth or tenth grade, who was not appreciative of me and kind of said that I shouldn't go and study.

Prof. Rosen: And you think it's because you were …

Prof. Goldwasser: A woman?

Prof. Rosen: … a woman, **(**and still are**)**?

Prof. Goldwasser: Yeah, I think he was like a chauvinist pig. [laughs]

Prof. Rosen: Okay. And do you think … like what is your opinion on the other women, the other girls in high school? They may have had a different experience than yours or you think there was something in Israel's society that was at the time?

Prof. Goldwasser: No, I think there were some girls who were really good at math and science. I think they were like … there were some girls who skipped the class, there were a few. We weren't many of us, you know when we went into the specializations. There was a class that specialized in math and science …

sorry, in math and physics, there were few girls, not too many. But they were very strong, so the ones who were there were very strong.

Prof. Rosen: And do you remember somebody in particular that went on and made a career in a related field?

Prof. Goldwasser: The truth is I don't know, I didn't follow them.

Prof. Rosen: Okay. Before we move on, any other figures from high school, friends, people that …

Prof. Goldwasser: Influenced me?

Prof. Rosen: … you remember influenced you, anecdotal stories?

Prof. Goldwasser: There are a few guy friends who went with me to high school who are now sort of well-known computer scientists.

Prof. Rosen: For instance?

Prof. Goldwasser: Yossi Matias. I think he's the head of Google Israel. Ehud Rivlin, who is professor in the Technion in computer vision. We were classmates. Yeah, so … But not only classmates, we were friends, we knew each other.

Prof. Rosen: So in the context of computer science, any other prominent computer scientists from the school?

Prof. Goldwasser: From that time?

Prof. Rosen: From the school, from the time.

Prof. Goldwasser: From the school, so I think that Adi Shamir actually went to that school, but he's older than me so he went there a few years before. And I think that Zvi Galil, who is now the head of the school of computing in Georgia Tech, he also went to that school, but again a different period. But they all had the same math teacher, this Uri that I mentioned earlier.

Prof. Rosen: I see. They also remember?

Prof. Goldwasser: Yes, yes, everybody remembers him.

Prof. Rosen: Everybody remembers?

Prof. Goldwasser: Oh yeah, he's a character.

Prof. Rosen: So it's safe to say that there was some influential figure there …

Prof. Goldwasser: Yes, absolutely.

Prof. Rosen: … that groomed them. So now US.

Prof. Goldwasser: Yes. Okay. So I arrive to the US, it's 1976. It's actually the Entebbe. As I landed in the US, it was really that day, and big excitement because the Israelis saved the day. I mean they saved almost everyone, this is … And I landed in the US. You know, Israel is like loved by everyone. I remember there was this beauty queen that was selected, the first Israeli beauty queen, became Miss Universe.

Prof. Rosen: Rina Mor?

Prof. Goldwasser: Rina Mor, right. But in general, '76 was a year of great admiration of Israel.

I land in the US and my brother comes and picks me up in New York, and we spend a few days in New York. Then we drive to … we take a bus to Pittsburgh, from New York to Pittsburgh, and … a new world. I knew nothing about Pittsburgh. I spent the summer in the dorms waiting for the school year to start. I actually never applied to the school. Just my brother told his professors that his sister is coming for a year and she's good at math. And since he was good at math and they knew that he was a talent, they said, "Does she want to come and study here?" and he said, "Yes," and they said, "Okay." And that was it. I became an undergraduate in mathematics, in applied mathematics.

But then it was applied mathematics and computer science. Now there's a computer science department undergraduate at Carnegie-Mellon. At the time, there wasn't. And the truth is that I actually loved studying. This was a revelation. When you go to high school, you sort of do what you're told, right? But I found it really interesting. I found the math interesting, I found the computer science interesting. I took this introduction class in Fortran programming. In the beginning, I had no idea. There were these cards where you put an instruction on every card and it goes through a machine and then it executes each instruction. I've never seen a computer before, I haven't really heard about computers before, but it was fascinating. It was really marvelous.

Prof. Rosen: Okay, I have two questions now, so I'm debating with myself. About the admissions, you said the admissions process was unorthodox in your case?

Prof. Goldwasser: I would say. [laughs]

Prof. Rosen: Now I want to ask what would have happened today with admissions?

Prof. Goldwasser: Ah, today. Today, no, the whole college admissions in the US is something bordering on insane. You know, there are standardized tests, there's grades, there's extracurricular activities, there are huge committees that sit and deal with every case. They accept legacy and people with talents that supplement whatever the needs of the school are, and who knows what else. And there's also a big mystery about this. All, in my opinion, geared toward making money on the admissions process. So, is the outcome any better? I believe serendipity is a big part of one's life trajectory, and maybe some of the serendipity's lost with this whole process that's very meticulous. But they're talking these days about having machine learning take over the admissions process, so we are in for a whole new era if that's going to be the case.

Prof. Rosen: Do you have any prediction where this may go, like specifically?

Prof. Goldwasser: I think it's the usual thing. When you start with a new technology, whatever it is – and in this case we're talking about something that is very disruptive, right? – we're going to have a machine that has access to a lot of data of the past decide who will be a good student and who will not be a good student, who's a match for Carnegie-Mellon versus a match for Berkeley versus a match for MIT and Harvard and so forth. My prediction is that in the short-term there will be a lot of mistakes until we understand what is being done. Hopefully if we are cautious enough and smart enough, we are going to be able to mitigate these mistakes in time so as to incorporate the things we really want before we sort of jump ahead and just kind of blindly let these algorithms make decisions that right now are done by individuals. Having said that, it's not that what's done by individuals is so perfect. So it's very hard to tell whether you are just actually doing better, because now you are treating this whole problem in a formal way, or you are doing worse because you are taking the human element out. But these are fantastic research problems.

Prof. Rosen: You have a personal connection to this kind of very such problem?

Prof. Goldwasser: Yeah, because my son is interested in it.

Prof. Rosen: Do you want to tell us about this now, or we can talk about it later?

Prof. Goldwasser: We can talk about it later.

Prof. Rosen: Okay, so I'll keep …

Prof. Goldwasser: Yeah, but my older son Yonadav, he's very interested in these topics of sort of policy, society, and machine learning. Sort of started from the machine learning, kind of a hard science, [0:50:00] and then he got interested in how to incorporate into them without sacrificing performance and utility. Also, these concerns that have to do with impact on the world.

Prof. Rosen: Okay, so maybe we'll get back to it later. Okay, undergrad years?

Prof. Goldwasser: Right. Undergrad years I'm in Carnegie-Mellon. I start in mathematics. There is this even program called Math Studies, which only a few kids go to, where there are these two professors who teach a handful of kids. It's supposed to go through all mathematics, you know, topology, geometry, algebra of course, and everything in two years, logic. And they spend essentially the first semester arguing with each other how to define each concept, definition … defienda, definiendo, back and forth, back and forth. It's abstract beyond anything that I've ever seen because in Israeli high school, things are very method-oriented. Right? They are teaching you how to perform, how to solve exercises. They don't really teach you … at least at that time, they didn't teach you about the concept of a limit or why are you taking derivatives and why you're integrating. Here, we are completely … it's all axiomatic.

So I go through this semester, maybe a year, and the whole thing is a two-year program, and after a year I quit. And I think to myself, "This is going to take too much time and I'm not the best at the class," and I decided I'm going to go and do computer science, sort of the computer science specialty within the math. And what turns out, so I take this class on I think set theory or data structures or algorithms, whatever, and it's trivial because my mind of course was so sharpened by this one year of dealing with abstractions and dealing with definitions that even if you don't think you're understanding them, you're completely in a different level. Then when you go back to something of a lower level, it's a triviality. This is an interesting experience that I have seen time and again with myself, with my kids. You push yourself to a place which is much more abstract and much more formal than maybe you care to be, and inevitably you start thinking more clearly, and you are able to sort of verbalize and conceptualize and define and understand. It's a fabulous discovery. Somebody has to prove a theorem about it explaining why is it they're being able to verbalize, why is it they're being able to define, and using precise concepts and precise thinking makes everything else simpler.

Prof. Rosen: So now you defend the very same thing that caused you to quit, like the abstraction?

Prof. Goldwasser: I know, I know. I mean in retrospect, maybe I should have stuck it out for another year, but that's what I did.

Prof. Rosen: It worked out well.

Prof. Goldwasser: It worked out.

Prof. Rosen: Okay, so then you moved to computer science?

Prof. Goldwasser: I moved to computer science. I remember a lot of my professors at Carnegie-Mellon. I remember Raj Reddy, who was … he taught AI. He was the founder of really speech recognition. At the time, it was the Harpy project. And I remember Anita Jones. She taught software engineering. She was one of my recommenders to graduate school later. So was Raj Reddy. And I remember there was another professor, Nico Habermann, who taught us compilers and I had a compiler project that I did with a friend. I remember we wrote this compiler which never compiled. [laughs] I remember writing this program for generating poetry. Today, they talk in machine learning about GANs, these things that can generate let's say poetry in a way that's indistinguishable from let's say poetry of a particular poet. But at the time, the way these programs generating poetry would work is that you would have some sort of a notion of a verb and a noun and how a sentence is structured, then you would have a dictionary and you would form a poem. I loved that.

Prof. Rosen: How large were the classes back then?

Prof. Goldwasser: The classes were small. I would say there were like about twenty kids. Again, very few women. That I do remember, that I was one of two and the professor also treated us a little bit with, you know, half … I was going to say "forgiveness," but "forgiveness" might not be the right word. A little bit, you know, like we were silly, even though we weren't really. And that, after I start doing very well in the class, he realized that. But that was my feeling. It didn't matter to me much because I didn't think of myself that way, but I do remember that.

I remember coming from Israel, my command of English was not perfect to say the least, and on every program that I wrote there always were these comments where he says, "Indent, indent, indent." I didn't know what word "indent" meant until the end of the term, but then I realized that "indent" meant that I was supposed to like, you know, indent the for loops and the different commands. So now I know what that means. But it was these silly things.

It was like, even I remember the first lesson of calculus when you come from Israel to America, and I remember telling my brother, who was in school at that time, I said, "I can't do this. It's too difficult." So he sat down with me. This is the first class ever in calculus, and he said, "Okay, so what didn't you understand?" and then it turned out that I didn't know the words "multiply" and "divide" and "integrated" and "differentiate." Then he told me what they all meant in Hebrew and I said "Ah." That was it. Then it wasn't difficult.

Prof. Rosen: Any other moments of despair and difficulty at that time?

Prof. Goldwasser: At that time? Well …

Prof. Rosen: You missed your parents?

Prof. Goldwasser: I missed my parents very much. At that time, you know in Israel somehow the idea of a phone call to the US, it was like an impossibility. It wasn't really an impossibility, but it seemed *so* expensive, nobody called. So I think I talked to them after one year on the phone on my birthday. And I missed them terribly, because I think in their mind I was capable of this journey, but really internally I was just a kid.

Prof. Rosen: So you didn't speak to them for a year you said?

Prof. Goldwasser: That's right, that's right. They wrote letters.

Prof. Rosen: Letters?

Prof. Goldwasser: And I wrote letters back and I wrote letters to my friends, but you didn't speak on the phone. Although I remember that a lot of the kids … when I did speak every once in a while, once a year or something, I remember that the kids in my hall in the dorms, they said … Again, it was like this girl who came from America in Israel, what I told you, in first grade. It was this girl who spoke on the phone and she was saying like, "Kha-kha-kha," which to them that's the Hebrew sound. [laughs] It's very guttural sounds. Yeah, that was hard, that was hard. Then I had to make a decision at the end of that year whether to go back to Israel to my army service, and I asked for a deferral, because the truth is that I actually kind of liked studying and I kind of wanted to continue. So I asked for a deferral of the army service.

Prof. Rosen: So it means that you skipped a grade or something? Because you were …

Prof. Goldwasser: No, I was just born early. I mean I was born in November. Somehow my enlisting date was late, so there was enough time there to actually finish a semester or semester and a half and then I ask for … maybe even a whole year, and then I asked for a deferral and they … You know, by the time the deferral came back, I was already finishing my second year. [chuckles] You know, I kept calling the embassy in New York and they said that I should wait until I get the answer. Yeah. So I finished my degree.

Prof. Rosen: What other difficult moments?

Prof. Goldwasser: Other difficult moments?

Prof. Rosen: Other happy moments also?

Prof. Goldwasser: Oh, lots of happy moments. I made lots of new friends and also I became a young woman, so there's also like personal relationships that you develop which happen when you are a young woman, and that regardless of

where you're at is very exciting, right? You're coming of age. And I came of age in Carnegie-Mellon during those years, between the age of 17 and 20.

Prof. Rosen: Okay. Just to be a bit more specific about those years, any particular topics that you related to, specific ones, beyond the aspect of … ?

Prof. Goldwasser: Yeah. I was very interested in AI. I was very interested in artificial intelligence at the time, I think because of the class that I took, because of this poetry generation, because of the whole concept of speech understanding and so forth, and also I think because this whole idea of understanding the brain and how we think and how we dream and why we dream, what we dream. That was fascinating to me.

So it was very clear to me when I finished that I would like to study this further. That's why I applied to graduate school. And I applied to graduate school at the same time that I applied for jobs, because I wasn't very clear about what I was going to do. There was sort of three options. In fact, this is the story of my life – there's always at least three options, sometimes four, but never one. And the options then were to go back to Israel or to go to graduate school or to get a job. The idea of going back to Israel was like I wanted to go back to Israel, but I was very afraid. Because at this point I was kind of distanced from the whole thing, and furthermore, I felt that I would like to go back to Israel, but at least I'd like to show something for all these years that I was away.

And I felt like I think a lot of people feel when they finish undergraduate school. At least I think they feel. That I knew nothing. Even though I studied for … I did my degree in three years in the States, although usually it's four. I studied during the year and I studied during the summers because I wanted to finish quickly so I could go back to Israel. At the end, you feel like, "What do I know more than anybody else? I want to own something. It'll be something that I'll understand [1:00:00] better than anybody." It's not even so much the idea of understanding better than anybody, but actually going into some subject in depth. At that point, it could have been related to artificial intelligence or algorithms. I remember also an algorithms course that was taught by Bentley, by Jon Bentley, and it was fascinating. I loved that as well.

So I wanted to know, understand something really well. I was told that there is this thing called graduate school. You have to understand, I didn't come from an academic family, it wasn't something that was standard, but …

Prof. Rosen: Did your parents have any degrees, your father?

Prof. Goldwasser: My father, because the war broke out when he did law school, I don't think he had a degree. He was the head of a few hospitals in Israel, and then he was an administrator in this health services. And my mother, as I said, was a home … she works at home, and …

Prof. Rosen: What about the ancestry? Rabbinical?

Prof. Goldwasser: The ancestry? Yeah, there is something there. My grandmother, they always talked about the fact that she had a golden *medale*, a golden medal in mathematics, when she was in high school and when she was studying maybe in school, after high school. But she didn't … she went … she came to Israel as a pioneer and they believed that they should work the land. They said the Jewish people should be connected to the land. But she has talent for math, because I remember that she loved it when I described to her math problems, and she surprised me because she actually understood and she could solve them. My grandfather had no idea. He was like a scholar, he learned with Bialik and Tchernichovsky, and he was much more of a humanist while she was into math. But in terms of being professors or academics, no.

In any case, I was told that there was this thing called graduate school. I think that like a day or two before, they said that I'm supposed to take this exam called the GRE. I didn't prepare at all, but I signed up and I went to the GRE. I didn't even know you were supposed to prepare, you know? It seems ridiculous how naive it was. So I took the GRE. I don't think I did very well. But in any case, I applied to graduate school and I got accepted to Carnegie-Mellon in engineering and Berkeley in computer science. First, I said to Carnegie-Mellon that I'm going to go there, and I went for the summer to RAND, to the RAND Corporation, where Raj Reddy actually recommended me as an intern. This was in Santa Monica, in California on the beach. And I remember this California. Wow. The beach. Fantastic, you know? I lived in Venice Beach and there's the roller skaters and the bikers and …

Prof. Rosen: Mellon …?

Prof. Goldwasser: So I was admitted to Carnegie-Mellon, which was the place I spent my undergraduate, and I was debating between the two, and I also had a bunch of job offers, but it was clear that I wasn't going to go get a job. I was going to go to graduate school. And I decided I'll go to Carnegie-Mellon. I mean I wasn't sure, but I decided I'll go to Carnegie-Mellon because I had friends there. You know, I had a boyfriend, whatever, you know the kind of things that people have, and friends.

But I had the summer job at RAND. And I went out to California with a friend, a woman called Sue Angebrandt that I did the compiler project with. She went out. Also she had some job in maybe TRW or something, a Jet Propulsion Lab, or JPL, or one of these companies near Los Angeles. And I was at RAND. And I remember that summer. I cannot tell you what I worked on, but I do remember that I was thinking to myself that the supervisors were all PhDs, and they were telling me what to do. It was some sort of AI-related project. I remember thinking

to myself, “Why should they tell me what to do? I should get a PhD and I should tell somebody else what to do.” [laughs]

In any case, so that summer was a fabulous summer. First of all, there was research and it was interesting, but I can’t tell you what it was about because I really have no recollection whatsoever. And second of all, all of a sudden it was … you know, I had an apartment of my own on the beach, it was California as I said before. You know, there were the roller skaters and the bikes. And then one day me and Sue, we decided to take a drive up the coast, up the California coast and go and see Berkeley, and go visit somebody that she knew in Palo Alto. I remember I had this small Toyota Corolla. Or Corona. Corolla I think. Some kind of car that they don’t make anymore. Maybe it was a Corona. Anyway, it was this little blue car, and we drove up the coast. And I remember driving into the Berkeley exit on University Avenue, and it was just blue skies that like you’ve never seen and the green hills in the background. I’m just sort of driving to campus. It’s such a glorious image. I can’t tell you … This is something you don’t forget. And it was “Wow, California, Berkeley.” Then I told CMU that I’m not coming and I told Berkeley that I’m coming, because it was just captivating.

Prof. Rosen: Without even going back to Pittsburgh?

Prof. Goldwasser: No, without going back to Pittsburgh.

Prof. Rosen: So then at the end of this summer you went to grad school?

Prof. Goldwasser: At the end of the summer, I went to graduate school at Berkeley and I started … I wanted to do AI, as I told you.

Prof. Rosen: What year was that?

Prof. Goldwasser: This was 1979. So I arrived at Berkeley. I had to find an apartment, the usual things that graduate students do. I live with a bunch of astronomer graduate students. In any case, I wanted to do artificial intelligence. At the time, there were few people at Berkeley doing artificial intelligence, but as I told you, serendipity is the name of the game. I was a TA, I had to support myself, so I had a teaching assistantship. Then I actually somehow got to work with Dave Patterson on the RISC project, Reduced Instruction Set Computer.

Prof. Rosen: Maybe you can tell a bit about that.

Prof. Goldwasser: About the RISC project? At the time, the RISC project was this idea of Patterson and other people at Intel at the time that the thing to do is to figure out which of the instructions I use most often, let’s say programs in Pascal and C, and those are the instructions that should be put in hardware in order to speed up computation. My part of the project was to figure out which instructions in fact are being used most often in Pascal programs. So I was quite

the programmer at the time. And I worked on this very large system, which I think adapted an existing Pascal compiler, a sort of thing that collects dynamic statistics, and I modified it sort of extensively to figure out which instructions should really be optimized or put in hardware. And that was my master's thesis, which I got at the end of that year.

Prof. Rosen: Did you enjoy it?

Prof. Goldwasser: It was Professor Powell and Professor Patterson. Did I enjoy it? Yeah, it was interesting. You know, it was a lot of work. It was very intense. This whole idea of being incredibly focused on a project and being in the office from day to night was borne at that time. I mean as an undergraduate, you spend a lot of time in libraries and studying for exams, but this idea that you have your own project and you set your own deadlines, although you know the professors expect things of you, it really comes from that time.

But at that time also, all of a sudden I wanted to go back … after I had the master's, I wanted to go back to Israel. I wanted to see Israel again. It's been four years. And I went for the summer. That was one of the highest … After four years not being in Israel, just being around here and with my mother and my sister. My sister was already a big girl. I remember taking a bus to Yamit. This was a time when they were actually returning the Sinai Desert. So I was in Israel then for three weeks, and then I came back to Berkeley and I continued to my PhD.

Prof. Rosen: This is after four years you haven't seen your family?

Prof. Goldwasser: No, my father came … No, actually my father came for graduation. That was after three years. And my mother and sister came after … You know what, I got the years wrong. My mother and sister came to Berkeley after four years. I went for this trip to Israel after five years. Yes, it was five years. So I did see them. I saw my father after three years, I saw my mother and sister after four years.

Prof. Rosen: That's not very often.

Prof. Goldwasser: No, that's not very often.

Prof. Rosen: Even for the time.

Prof. Goldwasser: No, yeah.

Prof. Rosen: Okay, so you finished your master's?

Prof. Goldwasser: And I got to tell you that I might be mixing it up. Perhaps they did come to visit me in Pittsburgh. But not, the quantas are like two years.

Prof. Rosen: It's the same order of magnitude?

Prof. Goldwasser: It's the same order of magnitude, yeah.

Prof. Rosen: Yes. Okay, so now let's go back to Berkeley.

Prof. Goldwasser: Yeah.

Prof. Rosen: And you finished your master's?

Prof. Goldwasser: I finished my master's.

Prof. Rosen: Is there something about the master, the time, the initial time in Berkeley that you recall that is worthy of mentioning?

Prof. Goldwasser: No. I remember the professors. There were the theory professors. There was Manuel Blum and Dick Karp and Gene Lawler. And I remember meeting theory students, the theory graduate students. There was Silvio [Micali], which later on became a very close friend and a close colleague of mine. There was Vijay Vazirani. [1:10:00] There was Faith Fich. There was Joan Plumstead. There was Mike Luby. They were all contemporaries of mine and I liked them. You know, I liked some of them more than others [laughs] as things are, and they're interesting characters. I took a class I think from Gene Lawler on scheduling, and I think his graduate … there was a TA there called Chip Martel. Anyway, and I did some projects on scheduling with Vijay and Silvio. I remember that.

Prof. Rosen: That was your first collaboration with Silvio?

Prof. Goldwasser: It was a project – right – in class. Yeah, that was the first collaboration. Then I met … I took a … I met Manuel Blum, and Manuel offered me to be his student. I spent the summer working with him, and that was fantastic because he was such an unusual thinker, and he wanted to work with me, or he suggested that I would be his graduate student. It was a huge compliment.

Prof. Rosen: You felt like it's a compliment at the time?

Prof. Goldwasser: Yeah, sure. It was a huge compliment.

Prof. Rosen: Who were his other graduate students at the time?

Prof. Goldwasser: I think that Vijay and Silvio were his graduate students. I think before that it was Mike Sipser and Dana Angluin, and we were sort of the new wave. There was the three of us, maybe Joan too, Plumstead.

Prof. Rosen: What was it about them that you liked at the time, do you remember?

Prof. Goldwasser: They were extremely intense. They really loved what they were doing. They would talk about this incessantly, but they were a lot of fun too. You know, Silvio was from Italy and Vijay was from India, and they were so colorful and they had fabulous sense of humor. And they went out to restaurants all the time and talked about work and told stories. It was really just somehow these were people of the world. So as much as I liked Carnegie-Mellon and had a lot of good friends, this was like a different dimension of personalities. If you think about it, people come to graduate school from foreign countries. They have lived a different life, each of them. They're older, they're sort of more worldly, and I was taken by it.

Prof. Rosen: Any particular memories, events from that before … ?

Prof. Goldwasser: From the period before research starts really?

Prof. Rosen: Yeah, before.

Prof. Goldwasser: Umm …

Prof. Rosen: Locations?

Prof. Goldwasser: Yeah. There is actually a memory or an event which I've told my younger son and I think it had effect on him, is that after about maybe like six months in or almost close to a year in Berkeley, I'm like a graduate student, I'm … Or maybe it's the second year already. I think it's the first year. I had a down period. It was like it's too hard and I don't have any original ideas and I'm never going to get through this, and I'm lonely, I don't know anybody, because I didn't have friends yet, close friends. And who do I think I am? And I was torturing myself continuously. What do I think about going to graduate school? Who do I think I am that I can just do this?

You know, I decided to leave Carnegie-Mellon where I had lots of friends and just kind of conquer this new place totally on my own. I remember going through this cycle again and again and again, and then I had this realization that okay, maybe it's all true. Maybe I will amount to nothing and maybe I know nothing, and maybe I'm a failure. But if I'm going to be against myself and I'm not going to be my own friend, then who else? I'm going to have to like myself whatever I am. I got to accept that. And somehow that was like a very kind of deep, decisive moment, that from then on, everything became better. Because I think it's very important to realize that for graduate students especially, which have moments like this, I'm sure it's universal, where you go, you've decided on this big adventure, and then it's very unclear, right? Are you going to succeed? Are you not going to succeed? There's a lot of competition. Everybody seems better than

you. And there's a I think tendency for self-beating, at least for some people, and it's very important to realize that it is what it is, you know you got to like yourself, because at the end of the day, "Ze ma yesh" (זה מה יש) *[Trans: "This is what you've got."]*

Prof. Rosen: And you never looked back? Like …

Prof. Goldwasser: Looked back at what?

Prof. Rosen: No, like you never had these thoughts again, they never recurred in your mind? Like the moment you decided, that was it?

Prof. Goldwasser: About my self-worth?

Prof. Rosen: Your self-, yes. Your self-worth and yourself.

Prof. Goldwasser: No, I've had them again.

Prof. Rosen: Okay, so we'll get to that then down the road.

Prof. Goldwasser: Mm-hmm.

Prof. Rosen: Okay. Any particular locations in Berkeley at that time?

Prof. Goldwasser: No, Berkeley was beautiful. You know, there was some restaurants that we really liked. There was a McDonald's at Berkeley. I remember meeting one of my graduate student fellows, Dan Gusfield, who was born in California, raised in California. I remember meeting him. It was right across from the McDonald's, which is the intersection of University and Shattuck, and he asked me where I was going. He was already a senior graduate student. I said I was going to McDonald's, and he looked at me like … he said, "Really?" I don't think he thought anybody actually eats there. But I came from Pittsburgh. You know, I like McDonald's. And it was like, "Well, you know it's a big chain. People do eat there." [laughs] But that was one more of those moments where I felt that I was different, and that I was right [1:15:27 audio cuts out for 4 sec] "better than thou" attitude toward the food, which I thought it was excellent. Of course, I don't think so anymore.

Prof. Rosen: Okay. When did that stop?

Prof. Goldwasser: I think that after many years that you don't eat McDonald's, you actually kind of get sick from it. [laughs]

Prof. Rosen: Okay. Grad school, research, Manuel Blum.

Prof. Goldwasser: Research, grad school, right. Manuel Blum. Okay. Manuel Blum took me as a student, but as things go, it takes time to find a research project. Then Manuel taught this class on algorithmic number theory. In this class, he taught us about first of all the basic elements of number theory, primes and composite numbers and quadratic residues and quadratic non-residues and generators and cyclic groups and all these things, and all from an algorithmic point of view. That is, how to test that a number is prime, how to generate a prime, how to find the quadratic residue, how to test that something is a quadratic residue, modular arithmetic and so forth, and always from an algorithmic and analyzing running times. I found it fascinating. I really loved it. I think essentially, I just have … You know, it's very basic. I like this stuff.

Prof. Rosen: I remember you teaching me this.

Prof. Goldwasser: That's right. So I really love this material. And at the end, he had a few lectures where he talked about cryptography. At that point, there was essentially RSA encryption scheme, which is a way, a public-key encryption scheme, which is a way to send messages between people who have never met before, secret messages. It all is based on the fact that it's hard to factor composite numbers which are a product of let's say of two primes, but it's easy to generate prime numbers. And that was nice. Then there was another lecture on another method by … There would be another method by Merkle–Hellman which Adi Shamir broke. And he did some cryptanalysis. That was interesting as well.

And then he asked the question, which was I think really defining for the rest of my career, and he said there is an Alice and Bob, and they are deciding to get a divorce. Alice is in Boston and Bob is in San Francisco, or vice versa, and they have to decide who gets the dog. And they want to be fair, so they decide to toss a coin, except they're not in the same place and they have to toss a coin over the phone, except neither one wants a dog. Or both want the dog, whichever is the case. And the idea that Alice just tosses the coin and then she says to Bob "It's heads," doesn't exactly work because they don't trust each other. So he asked "How would you do that? Can you use number theory to do that?"

So what's the connection? You know, why number theory? And that was sort of fascinating. Can you use sort of number theory? The idea that let's say factoring numbers is a hard problem and there's a public-key encryption to toss coins over the telephone.

And I start thinking about it, and I had an idea. The idea was at the time … I don't know if it's too technical for this interview. The idea for the time was that there was this function, which is exponentiation function, like $g^x \bmod p$. The idea was to essentially hide … for Alice to pick like a random x and send $g^x \bmod p$ to Bob and have him guess what x is. This is a function which is hard to … from g^x it's hard to find x. It's hard to invert. And he guesses some- … he tries to guess x, or actually to be more precise, he tries to guess something about x, like whether x is

odd or even or greater than a certain value *p* over 2 or smaller than *p* over 2. And he makes a guess, then she tells him what *x* is and she can check if the guess is correct or not. If the guess is correct, it's like heads has been tossed, and if the guess is incorrect, it's like tails. [1:20:00]

And Silvio and I talked about it. I told Silvio about this. Then you needed to prove something, right? You needed to prove that this is like a coin toss, that really it's impossible for Bob to guess better than 50-50 whether *x* was greater than let's say *p* over 2 or smaller than *p* over 2. And we had some proof, but there was a bug in it. And that was sort of the beginning of a lot of cryptography.

Prof. Rosen: Okay, so you're telling a story that is not related directly to encryption, that's one thing. Cryptography like is defined …

Prof. Goldwasser: It is related to encryption.

Prof. Rosen: It's of course related, but the story itself like is only anecdotally …

Prof. Goldwasser: Right.

Prof. Rosen: And I want to ask at this point how much context about cryptography did you have at the time beyond what Manuel … ?

Prof. Goldwasser: Nothing. Zero. Uh … Zero.

Prof. Rosen: Did you know about Shannon's work?

Prof. Goldwasser: Nothing. That was not part of the class. The class was about number theory and applications of number theory. I think that's what interested Manuel.

Prof. Rosen: Yeah, so why did Manuel Blum teach that class at that time?

Prof. Goldwasser: Because we're talking about 1980. Was it 1980 or 1981? And the invention of public-key cryptography was '76 I guess and then the RSA …

Prof. Rosen: Maybe you can give some context to the general … ?

Prof. Goldwasser: Right. So 1976, there was this incredible paper by Diffie and Hellman which suggested this idea that we are having this possibility of digital communication, that eventually everybody's going to be communicating with everybody else over the digital network. The is the case today. It wasn't the case in '76, but the possibility was there. And they were asking, "How can we utilize this in order to kind of shift the world into this mode of electronic commerce?" I think they even talked about these things explicitly in this paper. And they brought up these two possibilities.

One is what they call public-key encryption, which is a way for let's say an Alice and a Bob who've never met before to communicate secretly. Somehow there would be a directory where Alice would publish something that they called a public key, and Bob could read Alice's public key and use that in order to send her coded messages that only she, who knew also a private key, would be able to read, but no one else could. This was one thing.

Another thing that they suggested is this idea of a digital signature, which is that people could sign documents so that everybody can verify that Shafi signed it, but only Shafi could sign it. As you know, a handwritten signature, if I have a signature, it looks the same no matter which document I put it on. Here the case was that you would take a document and you would do a transformation to a new document which is called a signed document, and the ability to perform the transformation would be something that each user in the system, Shafi or Alon, could do in a way unique to them, because they knew some information or some private key that enabled them to do so and yet there was a matching verification key that would be able to verify that this was signed by Shafi or alternatively something was signed by Alon. In any case, they proposed these two things. They didn't exactly give ways to do it.

A year later, there was a paper by [Ron] Rivest, [Adi] Shamir, and [Len] Adleman where they showed how to do it using number theory. Around the same time, there was also a paper by Michael Rabin who showed yet a different way to do it also based on number theory.

And Manuel taught those three papers, because they were just mind-boggling. This whole idea, very tantalizing. Not only that, I think that Len Adleman – so it's Rivest, Shamir, and Adleman – was a student of Manuel's, so there was some affinity there as well. But one would have to ask Manuel why he taught that class. I think it was the first time he did teach that class, in any case. I think. You know what, maybe not. Maybe he has taught it before. Maybe, because there are these notes, these lecture notes on number theory by Dana Angluin. So he must have taught it before when Dana was a student, but I don't think he taught the public-key cryptography part of it.

Prof. Rosen: Who else was in the class besides you and Silvio [Micali]?

Prof. Goldwasser: Me, Silvio, Vijay, Mike Luby. You know, the usual suspects. I mean all of the crowd at Berkeley was there. Jeff Shallit was another good friend at Berkeley who … Eric Bach.

Prof. Rosen: They went on to do computational number theory.

Prof. Goldwasser: That's right. You know, that's right. Eric has this very famous paper about how to generate primes in factored form, which is an important

paper for generating generators for finite … for Z^*_P. Jeff Shallit also had very interesting work, and they have a book together on computational number theory. And we were all colleagues, and friends. And we're still friends.

Prof. Rosen: Okay, so now it begins?

Prof. Goldwasser: Now it begins. Right, so okay. So Silvio and I decided to work on the following problem, and the problem was how to play mental poker. Because there was one other paper that Manuel mentioned, and that was a paper by Shamir, Rivest, and Adleman where they used their encryption scheme in order to show how to play mental poker.

What is mental poker? People probably know what poker is, although I didn't because my parents didn't play cards and the whole idea of card playing was supposed to be this bourgeoisie thing that you did not do, that there were these families in Israel, that they played poker and they were considered, you know … somehow there was something improper about it. But again, this is my upbringing from a very kind of proletarian background.

Anyway, so this mental poker protocol by Shamir, Rivest, and Adleman, the idea is again, we are two players, we don't have a physical deck, we want to play poker over the phone, over the computer line, and how are we going to do that? How are we going to deal cards in such a way that you're going to get a random hand, I'll get a random hand, and once we get the cards they're not in the deck anymore without knowing what each other's decks are? They had an ingenious idea where there was a way to deal cards such a way that it wasn't obvious … I mean it seemed like you don't know what my cards are, that I did choose random cards, and same for you.

But [Richard] Lipton noticed that this protocol, there was a problem with it, that there was something about the implementation of this protocol that they proposed where it's true that you couldn't tell what my cards were, but you could possibly tell some information about my cards. For example, let's say that you could identify something was a high card versus a low card. So there was something about the encoding of the cards that did not hide all information about the card. Now for a card game, that's detrimental, right? If you know that I have a high versus a low card, that changes your strategy completely.

So the problem we set out to solve was how are you going to play mental poker hiding all partial information about the cards? I remember, so we're thinking about this problem and what do we need, and Silvio had this idea that we need to have some encryption scheme that … Not encryption scheme. We didn't talk about encryption. I think it was Silvio's idea that we needed a decision question, like a yes/no question, where it's hard to tell whether it's a "yes" or a "no" better than 50-50. But this was like an abstraction, right? And a little bit like the Diffie–Hellman …

Because I loved the number theory. I remember sitting in a seminar where some people were talking about something else, and in fact I must say that this repeats in my career over and over again. I get ideas while I sit in seminars when people talk about something else, which is probably a good reason to go to seminars. And all of a sudden, I had this idea about quadratic residues. I said, "You know what …" I think to myself that the way to encode the zero and one, the decision question would be to decide whether the number is a quadratic residue or quadratic non-residue mod, a composite number mod *n*, and this was a hard problem. I mean Manuel told us this was a hard problem, a hard problem in the sense that there were no efficient algorithms to solve it. And the reason why I thought it was a good idea is because it seemed to be a problem which is hard on the average. In fact, you cannot just tell whether something is a quadratic residue or non-residue, but you couldn't really do better than 50-50. And one would have to prove that, right?

But there was something about this problem, which is a notion that we … then later on to define formally, which is called random self-reducibility. It was sort of a way that if you had one number, if it was a quadratic residue you can generate lots of quadratic residue, or if it was a quadratic non-residue you could generate lots of quadratic non-residues. And then that means that if you could sort of distinguish one set from the other even a little bit, you will be able to distinguish whether your original number was a quadratic residue or a quadratic non-residue.

Prof. Rosen: How did you feel at that moment, or … ?

Prof. Goldwasser: That moment of thinking about the quadratic residuosity being the right problem and then telling Silvio? God, excitement. It's just incredible. Because pretty quickly, we could sort of come up with a proof.

And then, just to come back to the mental poker, the idea was that this would be a way to write down a card. Let's say the card is five of diamonds, okay. Then you write this down in binary, [1:30:00] the five of diamonds – so that's in zero/ones – and now you want to encrypt the zero, encrypt the one, encrypt a zero, encrypt a one, each time encoding it by a different quadratic or non-quadratic residue. Quadratic residue for zeros let's say, non-residues for one. You choose them at random. And now you have an encoding of the card, which is what we would call later probabilistic encryption or a randomized encoding.

Prof. Rosen: At the time, did you realize it's public-key encryption, or … ?

Prof. Goldwasser: We didn't even realize it was encryption. We had a card. We had a way to encode cards so that we could prove that there is no way you can distinguish one card from the next, because you couldn't distinguish zeros from ones better than 50-50.

Then we went to Dick Karp I think, because Manuel was on leave at MIT for a semester, and we told him about this. He asked us, “What about other partial information, not just with a zero/one?” These questions professors ask you are incredibly significant, because you don’t think this way, right? I mean now it’s an immediate question, but at the time it was a very fundamental question. And then we went away and proved that if you could tell any partial information – so you had to define what partial information would be, so there would be some sort of function of, you know, a string, any function of the string better than 50-50 – then you could actually reconstruct the individual bits of the card. Which implied that you could tell whether a number was a quadratic residue versus a quadratic non-residue, which was a hard problem.

Prof. Rosen: Can you tell something about the process of figuring out the right definition?

Prof. Goldwasser: The way I’m telling it to you, it’s really derived from the goal. The goal was to play mental poker in such a way that it hides all partial information. In order to do that, it was clear that you had to encode every bit individually, and furthermore it was clear that you would have to encode them in a probabilistic manner, because otherwise you couldn’t hide all partial information. Then there was that question of Karp’s, so we arrived to the question “What is partial information?” It should be any function that kind of divides the world of cards into … partitions them, because you’re not allowed to be able to partition them in any way. So any function that partitions them into sort of the left and the right, you know?

The process was just … it was like being in some kind of a mad state of creativity. And working with Silvio was just a very intense experience, as anybody who’s worked with him knows, any students. I mean there’s no day and no night. And I think he’s still that way. I’m not, but at the time I was. He was very intense, it was very exciting. And of course we didn’t do it completely in isolation. There were these questions that I’d say Karp asked us, and then I think maybe it was him or maybe we understood already there was a way to encrypt here, that it doesn’t have to do with card games. There’s a way to encrypt the zero and encrypt the one.

That’s something that was not known, because the public-key encryption of Rivest, Shamir, and Adleman or even the Diffie–Hellman concept, it really was intended of encrypting long messages which are unknown. And here zero and one, you know that everybody knows you’re either encrypting a zero or a one, but they can’t tell which is which. So this was a completely new way to encrypt information. We understood this is much bigger than it was, but …

And then we to consult people in number theory, you know, in math department. There was Lehmer and he was the expert. We were supposed to talk to him and

ask him, “Is it really the case that you cannot tell apart quadratic residues from non-residues? Maybe sometimes it’s not possible, but better than 50-50?” And I remember this quote. He said … We told him the whole story and we asked him what would he do if he needed to distinguish whether a number was a square or a non-square mod *n*. He said that if it was less than over two, he would bet it was a square. We asked him why, and he said, “Because there’s a lot of small perfect squares.” But he said, but he’s not a betting man. But then it turned out that this is okay because this doesn’t give much of an advantage.

Prof. Rosen: When you came to him, did you feel the stakes are high already, like … ?

Prof. Goldwasser: No. We came to him like as two young graduate students and he was very accepting. A little bit maybe I thought he was a little humorous, because it’s such a frivolous question, right? Playing cards, using quadratic residues. But I think the whole attitude of mathematicians to computer science has changed radically. Not to say that he wasn’t helpful. He was extremely helpful. But in general I think at the time, mathematics was this hard science and it was serious, right? And the whole computer scientists and the algorithm aspects and using it for cryptography was considered more of I think a toy activity. I think this is very, very different now. If I look at the mathematicians at MIT, and I’m sure it’s true all over the world, they have respect because we are studying hard questions, we are studying important questions, we’ve made impact on the world. Cryptography certainly has made a lot of impact. It’s making a lot of impact today. And only more so, as you well know as well.

Prof. Rosen: And I’m asking again about the stakes because I am curious to know, when did you realize how big your discovery is at the time?

Prof. Goldwasser: Right. So we realized that we have actually a scheme for encrypting single bits, something that was an open question that hasn’t been … nobody addressed it. And when you encrypt a single bit, obviously it’s going to have to be a randomized method, otherwise … because the public-key encryption, so everybody can encrypt zeros and everybody can encrypt one. If all encryption of zeros were the same, when you see the encryption, you can just yourself try to encrypt zero or try to encrypt one, and if it’s the same as what was sent, you know what was sent. So it has to be the case that there’s lot of encryptions of zeros and lots of encryptions of ones, and an adversary shouldn’t be able to distinguish whether we’re encrypting zeros or ones.

So here comes a definition – not to be able to distinguish the encryption of zeros and ones. That’s what we call semantic security. You cannot actually have any better than 50-50 plus non-negligible probability of success.

Now in the context of a protocol, okay, if you think about this mental poker example, not only that you’re encrypting the cards but there’s a lot of other

information going around. There's the dealing of the cards and there is many cards that are being encrypted. You could ask the question whether, having been part of this game, playing the cards, maybe you gain more and more knowledge as you go along so that now you are able to distinguish an encryption of zero from an encryption of one.

In order to prove that's not the case, we came up with this idea of a proof by simulation, the idea being is you say … well, let's suppose that your goal in the world really, you have no interest in mental poker, but what you want to distinguish is quadratic residues, quadratic non-residues. Okay? And somebody tells you that there is this mental poker game that's built on encoding cards with quadratic residue and quadratic non-residues, and they know how to cheat in this card. So what you say to yourself, "Okay, I'm going to show a reduction now. I'm going to show how to in some sense show that if in fact there is this person" – or this adversary, which we usually call them – "who is able to cheat in the mental poker game even by slightly better than he should, then there is a way to use this strategy and turn it into an algorithm that can distinguish quadratic residues from non-residues."

Since you believe that quadratic residues and non-residues cannot be distinguished in polynomial time, it means that such strategy does not exist. But how do you show such a reduction? In a sense you need to simulate everything, the entire view of the adversary – that is, the encoding of the cards and the dealing and everything that went on and was available to him to enable his cheating strategy.

This is what's called proof by simulation, which later has become a big paradigm in cryptography in how to actually prove security proofs. You can only prove security if you can sort of recreate the real world in which cryptography is used. And if you can simulate it, it means that it must have not have been that useful, because you could have simulated it anyway.

Prof. Rosen: In hindsight, you can view Shannon's security as being the information theoretic sort of analogue of semantic security. Did you see that at the time, or you came up … ?

Prof. Goldwasser: No, we didn't really know about Shannon's paper, because we were ignoramuses, [chuckles] which helped us actually. Shannon's information theory in fact, if you look at the definition, essentially says that the probability of two messages is the same given the ciphertext. That's one way to think of Shannon's security. An equivalent definition is the *a posteriori* and *a priori* probability of a message is the same whether you're give *a priori* without giving this ciphertext, *a posteriori* after giving the ciphertext. In other words, the ciphertext gives no information about the message. Or, if you think about the first definition, ciphertext for M0, which could be just a bit zero, or ciphertext for the bit

one, you cannot … there is no information in there that can tell you whether it was a zero or one.

If you think about semantic security, it's the computational analogue of it. That is, in principle, information theoretically you actually do have enough information to tell whether you're encrypting a zero or one, because it's a public-key encryption scheme, it's because the way the whole thing is set up. But computationally within polynomial time, you don't. If distinguishing quadratic residues from non-residues is a hard problem, if factoring integers is hard.

Of course, it could be that factoring integers is easy. We know that by quantum computers, factoring integers is easy. Then this whole tower of cards collapses. Fortunately today … This was the first probabilistic encryption scheme. [1:40:00] Today we have a lot of other problems, not just quadratic residues versus quadratic non-residues, not just the factoring problem, but problems on integer lattices. So problems essentially from geometry, where we can also sort of embed this idea of a decision question which is hard to solve and it's really impossible to decide the decision question better than 50-50, and we encode zero by a decision question where the answer is yes and one by a decision question where the answer is no. And these lattice problems, I mention them because they are right now quantum-resilient. In other words, we don't know any quantum computer algorithms that can solve them efficiently. They are what we call post-quantum cryptographic candidates.

Prof. Rosen: Okay, so at the time, the idea of basing something on an unproven assumption, it was in the air, it was kind of a bold move?

Prof. Goldwasser: Right. Well, if you think about RSA, they're also basing it on an unproven assumption. They are the first. They are assuming that factoring integers is a hard problem. We took another problem, which was distinguishing squares from non-squares. But obviously that's an assumption, and you know mathematics prides itself by having proofs, and proofs are proofs and not conjectures. So there's an underlying conjecture here, and that is that there's a problem which we don't know how to solve efficiently. But if you think about it, all of complexity theory is predicated on this idea that the class P of polynomial time problems and the class NP of problems which you can verify the correctness of the solution in polynomial time are disjoint *[ed: distinct],* so that P is different than NP. So to give meat to the entire field, there is an underlying conjecture which is widely believed but not proven.

Prof. Rosen: And at the time, what was the atmosphere? Did you experience any resistance to this idea?

Prof. Goldwasser: To this probabilistic encryption? We submitted it to a conference and it got in the first time. This was a conference in San Francisco. I think it was a STOC conference and I gave the paper, and the name of the paper

was “How to Play Poker Hiding All Partial Information & Probabilistic Encryption.” It was a long title. And I think that people were genuinely very positive, but speaking with people afterwards, I think they had no idea what I was talking about. [laughs] But certainly in the cryptographic crowd, there was excitement.

Prof. Rosen: Was it your first talk in the conference?

Prof. Goldwasser: Yes.

Prof. Rosen: And how did you feel?

Prof. Goldwasser: I felt on the top of the world.

Prof. Rosen: How well attended was it, just … ?

Prof. Goldwasser: Oh. In that time, the conferences were very well attended. There were no parallel sessions and people came to the entire conference, and it was a fairly small community. And it was very well attended.

Prof. Rosen: Can you tell us a bit more about the atmosphere at the conferences back then?

Prof. Goldwasser: I think that, you know, very intimate, very informed people. They were already people who were working on different fields – you know, algorithms and complexity theory, here’s a cryptography example and distributed computing. People started talking then about Byzantine Agreement. A lot of these big ideas that are still around as sort of fundamental problems were being discovered at the time.

Prof. Rosen: Were you attending all talks?

Prof. Goldwasser: Yeah, I was. Everybody was.

Prof. Rosen: And was it accessible to everybody, to a wider audience than it is today? How do you compare?

Prof. Goldwasser: I think so. But it’s natural. When a field is young and not overburdened by definitions and history and background, it’s easier to understand. On the other hand, people give much better talks today. People have learned how to simplify their talks – PowerPoint has helped quite a bit – and people have more respect to distilling the essence rather than giving all details. But, as in all things, there are better speakers and more speakers, and that hasn’t changed.

Prof. Rosen: Okay, so then you were … so you published in San Francisco?

Prof. Goldwasser: Yes.

Prof. Rosen: That was ’81?

Prof. Goldwasser: That was ’81.

Prof. Rosen: And what happened next? How did things evolve?

Prof. Goldwasser: ’81-82. Then, I had been to Berkeley at that point for three and a half years, and I had a very strong urge to get a job and leave. Somehow, I think about it now, I don’t know why it was so urgent to leave, but Berkeley seemed to me then like this small place and it’s time to go. I applied for a postdoc and I got a postdoc with Ron Rivest at MIT. I was there for half a year actually. Then they were looking faculty members and I started interviewing for faculty positions all over the country and also at MIT, and I got an offer for a faculty position and I started on the faculty in ’83.

Prof. Rosen: After having published what results at that time?

Prof. Goldwasser: There was this probabilistic encryption paper. Then there was another paper which we start realizing that it’s not just this particular quadratic residues versus non-residue, but you can take actually any function which is what we call a one-way function. That is a function which is easy to compute but hard to invert. And in particular the RSA function. We asked what bit about … The RSA function is you take an x and you take it to some power like x^3 or x^5 or x^e, exponent mod n. The question is “What about x is really well-hidden?” well-hidden in the sense that you can guess better than 50-50. So I did the paper on that, looking at the bits of x and showing, proving that they are as hard to guess as it is to invert.

Prof. Rosen: And this was still at Berkeley, or … ?

Prof. Goldwasser: This was still at Berkeley, yeah.

Prof. Rosen: With who was the paper, do you remember?

Prof. Goldwasser: This was Silvio and Po Tong, which was another graduate student. I think that those were the two papers that I had, yeah.

Prof. Rosen: Okay, and you got the assistant professor position at MIT?

Prof. Goldwasser: At MIT, yeah.

Prof. Rosen: And you moved there when? ’80?

Prof. Goldwasser: I think it was ’83.

Prof. Rosen: '83?

Prof. Goldwasser: Yeah.

Prof. Rosen: Okay, so you start as faculty at MIT?

Prof. Goldwasser: I started faculty at MIT and Silvio came a semester later. He was at University of Toronto and he also got a faculty position at MIT. It was like an incredibly intellectually exciting time. Oded Goldreich, who is now at Weizmann, came as a postdoc. There was Benny Chor, who was a graduate student there. Later also Yoram Moses came. I think Michael Ben-Or was there for some period of time. And all these people, they were young, they were brilliant, they were enthusiastic. We would work from day to night and then we would have dinners and talk about work and go to movies. And cryptography was starting to march along.

So I think that the next thing that I did was this paper on pseudorandom functions. The question was … There was an early paper by Manuel Blum and Silvio Micali on how to generate pseudorandom numbers in a way that you cannot distinguish these pseudorandom numbers from truly random. And the next question was how do you actually not generate just a polynomial-sized list of numbers but a very, very long list of numbers, an exponentially long list of numbers in a way that you could sort jump in the middle. Another way to think of it is a function. So …

Prof. Rosen: And what was the motivation for this specific question, given that you can generate a polynomially long … ?

Prof. Goldwasser: The motivation was that there are a lot of applications where you want to sort of random access. For example – I think this is one of the original motivations we had in the paper – so we called it an identify friend-or-foe system. We were saying, let's say that I in a group, we want to identify ourselves to each other, but there are some enemies that come along, and we don't want to use this password system where they ask, "What's the password?" I tell them what the password is, now they know. Instead, I want them to ask me a random sort of question, which I can answer. And if we are from the same group, they can verify my answer is correct, but anybody else, really as far as they're concerned it's a random guess. So if you think if you had what we call a pseudorandom function, there is a way for all of us who'll know the secret of this function or what we call the seed of this function to be able to compute this function f on any x, and then the random challenge would be x and I will tell you what f of x is. But being pseudorandom means that for anybody else, they can't tell it apart from a random function, so when they are asked x, f of x to them is like totally random. That's an application.

Prof. Rosen: So on that thread, I'm curious to hear how much of a role did practical motivation play in coming up with these notions?

Prof. Goldwasser: With these notions? That's a very good question, because it's not clear what you mean practical. When you say practical today, you mean there's going to be a startup that's going to implement it. No such thing, no startups. Nobody implementing. So the level of practical that makes any sense at that time is to say that there is a story, like identify friend-or-foe or people sending encrypted messages or people trying to authenticate themselves. And somehow I think those stories were important for narrative, because, as I told you, I've always liked stories, like the biblical stories. And in general I think people have an easier time to read, especially in a new field where there it isn't a mathematical problem that's been defined for many years and that people are interested in and they don't need any motivation. In a new field, you need to compel people, and stories are helpful.

But for us, it was really more of an intellectual story. The pseudorandom-number generator was just a polynomial sequence of numbers. Then the question about being able to kind of have an exponential sequence where you can sort of jump in the middle and just generate a polynomial number of them or this abstraction of a pseudorandom function is what interested us. And once you had it, you could tell a story, many stories.

Prof. Rosen: Did you feel any … So you didn't feel any pressure to practically motivate any of your … ? [1:50:00]

Prof. Goldwasser: No, no. None.

Prof. Rosen: None?

Prof. Goldwasser: No.

Prof. Rosen: And what do you think about this versus the alternative?

Prof. Goldwasser: Which alternative? That I had to practically …?

Prof. Rosen: Yeah. The need to find practical motivation.

Prof. Goldwasser: I think that every once in a while I have graduate students, and they come up with a question. For example, I have these two students now, they asked about pseudorandom functions, because what happens if you actually tell … somebody knows the secret of how to generate these pseudorandom values? Does it still possess some cryptographic hardness? This is a very technical question. But some of the reactions they got is that "What is the application?" And they came to me and they asked me if they should work on

it, they shouldn't work on it, what's my opinion, is it interesting? I said, "It's very interesting." It's intellectually interesting. They had a beautiful sort of approach to it. They had a beautiful proof. And at the end, that's the nugget, right? It's sort of something that captivates you, you have to use some ingenuity to solve it, and you have insight. And if it's important, even for applications, it will emerge, but it's not necessarily obvious in the moment that you start. And sometimes if it is very obvious, first of all lots of people work on it, and you know competition is good but only to a certain extent. If everybody's working on the same problem, there's some kind of … I don't know. I don't like to be in a space that's very crowded.

Prof. Rosen: How did it feel back then in the early MIT days in terms of competition?

Prof. Goldwasser: Right. As I said, we were a big, happy family, but [laughs] a big, happy family of a lot of people who wanted to do well. So we worked collaboratively, we've got a lot of joint papers, also with Benny on this thing called verifiable secret sharing and with Oded on pseudorandom function. But we each started, within a couple of years everybody started going in their own way as well, because you are in an academic system, they compare you, they promote you at different times, they tell you that you should kind of shine individually. And I personally …

Prof. Rosen: How was …

Prof. Goldwasser: You asked how did I feel. Remember we talked about the crisis of becoming a graduate student. That was again a time which was extremely difficult, because you're trying to do something new, you're trying to do it on your own, you are always comparing yourself to the people around you who are always brilliant, and more brilliant than you are, and you don't know that they're all feeling the same thing. You know this imposter feeling? Apparently they're all feeling it. Some of them admit it, some of them don't admit it. [laughs] But once you realize that this is the name of the game, I think again it's these moments of realization.

Prof. Rosen: So did you have such a moment?

Prof. Goldwasser: Yes, yes.

Prof. Rosen: When was that?

Prof. Goldwasser: I think I was talking to somebody and they told me about this imposter … I told them about how I feel and they told me about this imposter syndrome. Now everybody knows it, but then I never … I asked what it was and they explained, and it was like, "Ah, okay."

Prof. Rosen: That was person external to the … ?

Prof. Goldwasser: Yeah. Like a friend, yeah.

Prof. Rosen: Okay. What about teaching? Do you have any memories?

Prof. Goldwasser: Yeah. Teaching we really started … I started and then Silvio also together teaching this class on cryptography. It was the course of Manuel Blum but with a lot more, because at this point the cryptography was a big part of it. There was the definition of bit security and the semantic security of an encryption and the mental poker, and the partial information, pseudorandom functions, pseudorandom number generator. It started being a field. And we haven't talked about zero-knowledge yet.

Prof. Rosen: That was before zero-knowledge?

Prof. Goldwasser: Around the same time. It was before it got in, but …

Prof. Rosen: Before we get to zero-knowledge, who were the students in this class that you remember?

Prof. Goldwasser: The students, yeah. There was Johan Håstad, there was Joe Kilian, there was Bill Aiello. I think in the early years there was Yishay Mansour, but I think he was a little bit later. Those are the students … there's Paul Feldman, who was a student of Silvio's. The others were student of mine. And they're all big names, fantastic researchers in their own right.

Prof. Rosen: How did the other MIT faculty treat the young field of cryptography? How did they perceive it?

Prof. Goldwasser: MIT is an incredible place. I think that they really have had the foresight of hiring people who were not necessarily in the mainstream of theoretical computing, but sort of doing something with the tools of theoretical computing which is a little bit on the fringes. Rivest was like that. Public-key cryptography after all was exciting, but it was unusual, right? And Silvio and I certainly, and Charles Leiserson was doing also things which were, you know, with applications. At that time, I think it was data structures and stuff like that. Nancy Lynch was doing distributed computing and Byzantine Agreement and lower-bounds [on] Byzantine Agreement.

So I felt that they were incredibly proud of all achievements, and especially Ron Rivest, who was a major mentor. Because now that I think of it, he wasn't really much older than we were. Maybe 5, maybe 10 years, no more. And he was extremely supportive of us. I have a paper joined with him, digital signatures. But by and large, we each did our own thing, and I think Ron started working on computational learning fairly quickly, so he kind of left the cryptography field and did that sort of in a more commercial setting for a few years.

Prof. Rosen: And the story about the writing of the Goldwasser–Micali–Rivest paper in two hours, is it true?

Prof. Goldwasser: [laughs] In two hours, no. It's the talk. Ron was giving a talk in a rump session about this. We had this idea and we worked on it, and then I told Ron, or maybe Silvio and I told Ron that he should give a talk in the rump session. So in the Crypto conference, there are these 10-minute or 5-minute presentations, and he just sat there and he wrote his slides and they came out so eloquent. I mean he's really remarkable. Yeah.

Prof. Rosen: What other faculty do you remember from the time being supportive?

Prof. Goldwasser: Albert Meyer was very supportive. I remember this first award, that he put me up to the Grace Murray Hopper Award. I think he was really a very significant mentor in his own way, sort of in the background. I mean Ron was in my field, so it was sort of more of a daily advice or monthly advice. But Albert was at the head of the theory group and he saw something in me and put me up for this award, which made me feel good, made me be recognized.

Prof. Rosen: Okay. Is it time for zero-knowledge?

Prof. Goldwasser: Yeah, I think so. So zero-knowledge. Alright. So this whole idea of having a protocol where let's say two people are sending messages back and forth and there's a goal for the protocol usually. The goal might be to … In the context of going back to that mental poker, say you want to prove that the cards that you encoded were encoded property, but you don't want to say what the encoding was. So there's a statement here, and that is that all 32 … sorry, all 52 cards have been encrypted and no two cards are the same, but you're not going to tell me which card is which. Then there is apparently a way to do it. Apparently. We showed a way to do this, which amounts to actually showing whether something is a quadratic residue or a quadratic non-residue, so that I can prove to you that something is a quadratic residue or that something is an encryption of zero, or let's say the two things are encrypting different bits, in such a way that you will have learned nothing else.

Prof. Rosen: So you had a protocol?

Prof. Goldwasser: So we had a protocol. And now we had to have a definition. What does it mean, prove so that you learn nothing else? The definition went back to the simulation paradigm. Sort of we had this definition which said that a proof or a protocol with zero knowledge to whoever I'm proving it to … So I'm a prover. I know something and I'm proving it to you. I'm proving you some mathematical statement without actually giving you the proof, which seems a bit weird, so at the end you'll be convinced that the statement is correct. But what do

I want? I want you not to be able to prove it to a third party. In fact, I want you to learn nothing from it. So how do you define it? The way you define it is that whatever you could have computed before you interacted with me, that's no different than what you can compute after you interact with me. And an equivalent definition to that is that you could essentially simulate the entire interaction between us. And if you could indeed do so, it means that interacting with me was useless to you, assuming the theorem statement is correct.

Prof. Rosen: And the name "simulator," when did it come about?

Prof. Goldwasser: Who remembers.

Prof. Rosen: At what stage? There's a story about multiple rejections?

Prof. Goldwasser: Ah, okay. Right. So this paper, we started. We didn't actually call it "simulation" I don't think. I think it had some other definition. They were many names for this paper. It started, it was "Participatory proofs … " "Interactive proofs such that they hide all partial information." There were many, many names until we got to the final name, which was "Interactive proofs and zero knowledge" or "The Knowledge Complexity of Interactive Proof." And the paper was rejected like 6-7 times. God knows. But we were very persistent, you know? [2:00:00]

Prof. Rosen: How did you feel with each rejection? What's the **…**

Prof. Goldwasser: Well, you know there were three of us. I mean in the beginning there were two of us actually on this paper, Silvio and I. And then Charlie Rackoff joined. He improved the paper, but it also got rejected. Because there were three of us, we could sort of build each other up. And how did we feel? We felt like everybody else was an idiot. [laughs]

Prof. Rosen: So you …

Prof. Goldwasser: What?

Prof. Rosen: You had this confidence back then that you're onto something?

Prof. Goldwasser: But this concept was so interesting and we liked them, and it was clear that this is a great paper.

Prof. Rosen: And Charlie Rackoff was at the time where?

Prof. Goldwasser: He was in Toronto.

Prof. Rosen: In Toronto, so how did the interaction work back then?

Prof. Goldwasser: I think Silvio and Charlie interacted when Silvio was in Toronto. They had some paper on coin tossing or something. Then Silvio came to MIT and we continued working on the interactive proofs, but I think there must have been some interaction between them. I wasn't … It really wasn't a three-way interaction.

Prof. Rosen: But how was communication with people from other institutions working in general?

Prof. Goldwasser: Well, there was email, but there certainly wasn't the World Wide Web, or it wasn't immediate. There were phone calls, a lot of phone calls. There were visits.

Prof. Rosen: Do you remember any notable visits, visitors and/or visits from the time or from … ?

Prof. Goldwasser: At MIT?

Prof. Rosen: Yes.

Prof. Goldwasser: Adi used to come to work with Ron. Again, I told you that Oded Goldreich was around. And that's about it.

Prof. Rosen: Okay. So zero-knowledge was rejected and you said the manuscript improved over time with the rejection?

Prof. Goldwasser: It did improve over time. Sort of in the beginning, I think the simulation was under computational assumption, then it became without an assumption. Finally, it got in. We were mighty happy. And we went to the conference. I'm trying to remember who gave that talk, if it was me or Silvio. I don't remember. But in any case, at the same time, at the same conference there was another paper, which was called "Arthur–Merlin Games." This was a paper by Babai, who introduced this concept …

Prof. Rosen: And Moran also.

Prof. Goldwasser: And Moran. Who introduced this concept where there was a prover and a verifier like we had, except the prover's name was Merlin and the verifier's name was Arthur. And the difference between a verifier and Arthur was that Arthur was just tossing coins, he was very naïve, and Merlin then, based on Arthur's coins, he would kind of teach him things or prove to him things, such that if he was proving a correct statement, Arthur would believe it, which we call completeness, and if he was proving an incorrect statement, it doesn't matter what strategy Merlin would employ, Arthur would not believe it. That was the same as interactive proofs, except our verifier didn't just toss coins. He tossed

coins and did computations, and based on these computations would send messages.

Prof. Rosen: And their motivation was totally …

Prof. Goldwasser: Their motivation, there was some group-theoretic problems that they wanted to show were in NP, but they couldn't, so they allowed the … in NP, you also can think of it as a proof system where there is all powerful prover and he writes down a string which is a short proof that can be checked in polynomial time. An interactive proof, it can go back and forth, back and forth, so the prover can send the string, the verifier asks the question based on some coin tosses, the prover sends another string, go back and forth, back and forth, and in the end the verifier says, "I'm convinced."

Prof. Rosen: So essentially in your paper, there are two main …

Prof. Goldwasser: So what I'm saying is – sorry, just to finish that thought – is that what Babai was trying to show, some problem, some group-theoretic problem was in NP, but he couldn't, so what he did is he added this Arthur that was able to toss coins. And for an Arthur that could toss coins, there was a short interaction by which you could show some group membership problem.

Prof. Rosen: And when did you realize that it's a similar related concept? At the conference? Was it at the time of the conference?

Prof. Goldwasser: I think it was at the conference.

Prof. Rosen: And did you already realize back then, view it as a generalization of proof systems?

Prof. Goldwasser: Yeah, we did. I don't know if they did, because for them it was really a system to show a complexity, the complexity of certain problems. They defined a complexity class and showed that they had problems in the complexity class. For us, it was always the case because we were coming from the cryptographic setting. So there were parties. There were these Alice and Bob, where Alice was the prover, say, and Bob was the verifier.

Prof. Rosen: No, but there's a complexity point of view and there's a cryptographic point of view. There's the interactive proof and the zero-knowledge proof.

Prof. Goldwasser: No, but what I mean about interactive proof is that there was a story, there was a prover and a verifier. And regardless of whether you would think of them as cryptographic agents or not, the prover's goal was to prove a statement and the verifier's goal was to verify a statement. So it was a proof system. Then the class was all those statements or languages where you can

prove membership in the language or correctness of the statement via such an interactive proof. Yes, so we did understand.

Prof. Rosen: To what extent did you understand the important open problems that emerged from this new concept at the time?

Prof. Goldwasser: Yeah, they were abundant. One question was whether this system of Babai and interactive proofs were the same. He had this system of Arthur–Merlin. We had this verifier–prover. Arthur could only toss coins, the verifier could actually toss coins and compute on them, and that seemed to be a very important feature that enabled you to prove things you couldn't do just with coin tossing. So that was a clear question.

Then Mike Sipser and I, we proved that those two classes were the same. Interestingly, it all started again from the quadratic residue question, which was a question that kind of followed my career, because it seemed like to prove that something was a quadratic non-residue required, without sort of revealing information, required a verifier's power to hide the results of his coin tosses. And I was talking to Mike about this, and then he had this idea that we could look at the set of all quadratic residues and the set of quadratic non-residues, and talk about what are the union of those sets ... Anyway, we talk about size of sets and relate that to the question of whether a number was a quadratic residue or quadratic non-residue, which is related in turn to the question whether Arthur–Merlin games and interactive proofs are the same class or not.

Prof. Rosen: Did you have any applications in mind beyond the original mental poker application?

Prof. Goldwasser: Not really. It was again a concept. How do you prove a theorem in such a way that you will believe the statement but you will learn nothing else, with the definition that I gave you, and that you won't be able to prove the theorem to a third party?

But very quickly after, as soon as the paper came out, Adi Shamir pointed out the application for identify theft. Here in this situation, you would think about me. What identifies me is the fact that I know how to prove some theorem and nobody else knows, because it's a difficult theorem to prove. But I have the proof. How do I have the proof? Maybe the proof is something like I know the factorization of some number. How do I know it? Because I took two primes and I multiplied them, so of course I know how to factor it. Now I want to prove to you that I know this factorization or something about this factorization that only I will know. That would identify Shafi, that there's this composite number and she knows how to factor it. He realized that this is an identification method, and he took actually a protocol that we have for proving that something is a quadratic residue and made it more efficient sort of in terms of how many rounds you need

to accomplish it, and it … This is work with Fiat and Shamir, and this became an identification scheme.

But the interesting thing about zero knowledge is that is really the tip of the iceberg. Really, "the tip of the iceberg" is the wrong analogy. In any case, that's just scratching the surface, because it turned out that even though we showed the definition of zero knowledge in applications of zero knowledge in the sense of particular number-theoretic questions you could do in zero knowledge, like whether something is a square or a non-square, it had a much wider applicability.

There's a follow-up paper by Silvio Micali, Oded Goldreich, and Avi Wigderson where they showed how to prove that a prover can prove to a verifier that a graph is three-colorable, and that's an NP-complete problem and it follows from this is that you can actually show any NP statement in zero knowledge. So I can prove to you any statement that has a short proof in such a way that at the end, you'll believe the statement but you will have no idea of the proof. In order to do that, they introduced computational assumptions, so this was under the assumption that one-way functions exist.

What this means – okay, going a little bit into the field – is that essentially we can take now any protocol, any protocol between let's say multiple people, not just two, let's say *n* people, where there's a program say that specifies what messages I'm supposed to send to Alon and what messages Alon has sent to a third party and so forth. The thing is that the messages that I'm supposed to send are based let's say on my passwords or some private information I have. The messages you have, you're supposed to send are based on what you have received from me and your private information. And I don't … So I do my computation, I send the message. If we're all honest, everything's fine.

But suppose I'm a liar. I'm an adversary. We're in a cryptographic setting. We're all liars in some sense, or we have to protect ourselves in any case. How do you know I'm sending the right message? How do you know I did the computation correctly, based on this current time, based on my private information and all the messages I receive, the next message I send is correct? Well, that's an NP statement, right? So there's a statement to prove, and that is that I am sending the correct statement. If I can prove that in zero knowledge, it means that I can actually transform all protocols that work when people behave properly to protocols that work [2:10:00] when people behave improperly, because essentially every message I send is accompanied with the proof that that is the correct message, and it's a zero-knowledge proof so I'm not revealing anything about my secrets.

Prof. Rosen: What about other applications?

Prof. Goldwasser: Lots of other applications. The next application is something called multi-party computation, which is a little related to what I just said, but it's

actually much more relevant to today. So let's talk about the fact that we are now living in this data-driven society and different parties, it might be different hospitals or different national agencies, and they have a lot of data. If you think about hospitals, it could be one hospital has my genomic information and another hospital has my blood type, my blood test over the years. Another hospital might know something about illnesses that I have experienced. And they would like to share … they would like to compute something based on this data, but they don't want to reveal to each other the data. Another example might be that I am the tax authorities and you are the immigration office and somebody else is, I don't know, another governmental agency. And because of regulations, they're not allowed to share their information. Still, they would like to compute some function that's based on all of the data together.

That's what we call multi-party computation. There's multiple parties, each one has data which is confidential, and they want to compute some function that depends on all the data without revealing it to each other. It turns out that it can be done. And it can be done partially … there's a little bit of algebra involved, it's beautiful theory, but what does zero knowledge have to do with it? If everybody's honest, it can be done. It's an interesting method of how. But what if somebody's not honest? Maybe they're not following the protocol. Well, you just tag on zero knowledge to each one of their messages, and then even if they are potentially dishonest, you will be guaranteed correctness because they will be caught if they deviate from the protocol.

Prof. Rosen: Did you foresee the generality of the method at the time?

Prof. Goldwasser: No, no. It's way …

Prof. Rosen: Nothing? Again, you were m- …

Prof. Goldwasser: … way beyond its time. I mean ahead of its time.

Prof. Rosen: And again, what was the reaction back then?

Prof. Goldwasser: About multi-party computation?

Prof. Rosen: Yeah, to these new revolutionary ideas.

Prof. Goldwasser: First, there was a paper by Goldreich, Micali, and Wigderson, who did this multi-party computation based on the existence of one-way function. That got in. I think it had strong reaction. I mean good reaction. But then there was a follow-up paper that is by myself, Micky Ben-Or, and Avi Wigderson which happened at a time that I was visiting Hebrew University on sabbatical, and that did not have computational assumptions.

So there's sort of a partition, a crowd within I think theoretical computer science, and maybe less so these days. Some of them are so intrigued by the concepts and they're willing to make assumptions like the existence of one-way function or that it's hard to factor integers and so forth. Some, that discounts results for them, so when you can prove an information-theoretic result without assumption, they're happier. So I think that the fact that there were information-theoretic analogues was very helpful for this whole theory to be adopted.

Prof. Rosen: Okay. Before we move on, I'd like to ask more about applications.

Prof. Goldwasser: Okay.

Prof. Rosen: Digital signatures. Fiat–Shamir you mentioned.

Prof. Goldwasser: Yeah.

Prof. Rosen: So maybe you want to talk about that?

Prof. Goldwasser: Actually, I want to say something more about zero knowledge.

Prof. Rosen: Okay.

Prof. Goldwasser: So we've mentioned like this. First, it was intellectually curious. Then Adi … Fiat and Shamir realized this is important for identify theft. Next step was that this enabled a conversion of protocols from honest parties to potentially misbehaving parties. But then all of a sudden in recent years, it had some very unusual usages. One of them was by some researchers in Princeton together with Boaz Barak where they talked about the use of zero knowledge for nuclear disarmament. Now it sounds like, you know, out of nowhere. The idea there is that you want to be able … let's say the Russians and the Americans want to make sure that they are disarming nuclear warheads, but they don't want to show each other the technology. How do you prove that a nuclear warhead is in fact a nuclear warhead without looking inside? It sounds like you want to prove a statement but give zero knowledge. And it's not just by association. There's actually a concrete method that they use which uses a lot of underlying principles from the mathematics of zero knowledge.

Another example, which Moni Naor from Weizmann came up with, is suppose you are a suspect in a crime and you want to prove that you did not commit it, so they are asking you to give some DNA so that they can compare it to the forensic. The point is you don't want to give it because maybe you are planning on doing a crime in the future or your children are. So how do you prove that you were not in the crime scene, or your DNA does not match in zero knowledge without actually giving the DNA?

So there's all these applications all over the place. The last application is the blockchains. Today, as you know, there's this whole idea of Bitcoin, blockchains, how do we put transactions out on a blockchain so that they are serialized in time? And some of the questions are, okay, so you want to put transactions, or transactions meaning things you've done, you want to have records that everybody can see. But sometimes you don't want everybody to know the details of the records. You might want to prove that two records are the same, or other properties of the records, and you want to do that in zero knowledge. So it has actually become very well known to people in the trade these days and there are even companies that specialize in zero knowledge.

Prof. Rosen: And also digital signatures?

Prof. Goldwasser: Yes, digital signatures. Yes. So what are you asking about that?

Prof. Rosen: Fiat–Shamir, the standards digital signatures over the web is based on ideas going back to zero-knowledge, the ones that started in the late '80s.

Prof. Goldwasser: So digital signatures were invented, as I said, in Diffie–Hellman's paper. Then RSA had implementation, but there was really no definition of security. So obviously you don't want it … a digital signature should be secure, it shouldn't be forgeable. But then we came up with this definition for what does that really mean? So what would that mean? Let's say someone's a notary public, so they're able to sign. You want to make sure that even though you can go to the notary public and give him documents at will for them to sign, that you are not able to learn how they sign and be able to sign a document in the future. This is what we call digital signature secure against chosen message attack. In other words, I can choose the documents that I feed the notary public to sign and yet, even though I see polynomial number of signatures, I'm not able to produce yet one more document for which I sign it without the help of the notary public.

Prof. Rosen: And you came up with the first definition of what this means.

Prof. Goldwasser: Definition and construction, we had a way to do it.

Prof. Rosen: And then eventually it became crucial to the development of electronic commerce over the Internet.

Prof. Goldwasser: Absolutely.

Prof. Rosen: Okay, so moving onto information-theoretic and unconditional results. Maybe first we talk about geographically, where are you located now, your area?

Prof. Goldwasser: Yeah, so this is 1986 and I … Actually, we should talk about primality then before.

Prof. Rosen: Right. So let's talk first about primality?

Prof. Goldwasser: Yeah. Okay, so as I told you, interactive proofs, or maybe I didn't mention it, but we were talking about the fact there's a prover and there's a verifier. The verifier's tossing coins. They go back and forth. The big distinction of interactive proofs from classical proofs is that there is a probability of error. I proved to you something and with very, very high probability you know it's correct. Or another way to say that, there's a very small probability that I managed to cheat and prove an incorrect statement. That's what enables zero-knowledge.

So, as I told you, I was always interested in number theory, and there was this problem around, which was how do you test numbers for being prime? And a beautiful old result by Miller and Rabin and Solovay and Strassen is an algorithm for testing numbers whether they're primes or not, a fast algorithm that has a probability of error. So at the end, you run this algorithm, you know with very good probability that your number is prime. In fact, what it is, is that if it's composite, you're likely to detect that it's composite, and if you don't detect that it's composite, you say, "It's probably prime." So an interesting question was can you have a primality test that doesn't have any probability of error? Can we test that a number is prime or composite and be a 100% correct? And can you do that without actually factoring the number? That was work that I really enjoyed tremendously and did with my graduate student Joe Kilian at the time.

Prof. Rosen: That was your first graduate or was it the … ?

Prof. Goldwasser: Joe? No. Johan Håstad was my first.

Prof. Rosen: Johan Håstad?

Prof. Goldwasser: Yeah.

Prof. Rosen: And do you want to tell us more a bit about …

Prof. Goldwasser: About the story?

Prof. Rosen: … the story?

Prof. Goldwasser: Yeah. I was in a conference again. As I told you, sitting in lectures really works well for me. I was in a conference in Arcadia, it was some conference center there, and Schoof gave a talk, [2:20:00] René Schoof gave a talk about some algorithm he had for taking square roots mod *p* for small

numbers. It had something to do with elliptic curves over finite fields, which was something I knew nothing about, but he described what an elliptic curve was and he had some algorithm for counting how many points are on a curve. And this whole elliptic curve was defined with respect to a prime. So there was some equation, you know, *y*, *q*, whatever. y^2 is equal to x^3 plus *ax* plus *b* mod *p*, and you could count the number of solutions *y, x* in this defined group, and he was doing some operations on the group.

In any case, he had an algorithm. And when I was sitting in this lecture, I started thinking to myself, "What if you'd run this algorithm but you … mod *p*, except you didn't know whether *p* was a prime or composite? How would the algorithm perform? Would it work? Would it not work?" And I asked him that question. I think it sounded like a really weird question and he was like, "Well, it probably would be garbage if you ran it mod *p* where *p* was composite."

So then I went back to Cambridge and I think I invited Schoof to come and give the talk at MIT. And he came and gave the talk again, so I understood a bit more. Then I start talking to Joe about the question of what if this prime was a composite, and we start talking about how to use these elliptic curves working mod a modulus which we're trying to tell whether it's a prime or composite, and then the rest is history. We had a primality test based on elliptic curves where at the end, it was randomized but there was no error probability.

Prof. Rosen: That was in '86?

Prof. Goldwasser: That was in '86, yeah.

Prof. Rosen: Okay. And then what?

Prof. Goldwasser: Then what? So then just, you know, it was '86 or '87 and I haven't been in Israel for many years. I used to come visit, but I was really pining away in some sense to being in Israel for some extended period of time. And I had a sabbatical and I decided to spend it in Israel.

[Ed. - This paragraph recorded at the end but moved here.] So when I came to visit the Hebrew University, that was in 1987. It was an incredible visit because I haven't been in Israel for a long time prior, and it was incredible personally because I met my husband here, Nir Shavit, and it was incredible scientifically as I will … as I have described to you.

And I came to the Hebrew University and there, there was Avi Wigderson and Nati Linial and Benny and Michael Ben-Or. I didn't know what I was going to work on. I was teaching a course about primality and elliptic curves, and they were very excited because elliptic curves were creatures that they didn't use in computer science. They haven't been used that much either since, but in any case, I was teaching this class.

Then I remember that I was in Avi's office and they asked me this question. He says, "What else is there to do in cryptography? Because we've already done encryption and we had like good definitions and signatures and identification schemes and zero knowledge, and what else is there?" So this is a question for some reason people ask many times, many years later. At that time sort of under the pressure of the moment, which was always very good for me to be asked questions under the pressure of the moment, [laughs] it's an aspect, it was like "Well, you know, we make assumptions, and maybe we could make some sort of physical assumptions rather than computational assumptions like that factoring is hard, and we could prove results absolutely."

Somehow that conversation led to two different papers. One of them was, when I told you about interactive proofs, I told you that there was that result that said that you can actually prove any statement in zero knowledge using an interactive proof if one-way functions exist. If you like, if factoring is hard. And that's a conditional result, right? So one question is, can you do it without any assumptions? Well, what we came up with at the time, and this was with Joe Kilian also, was this model where there wasn't a single prover and a single verifier, but there were two provers. Now that sounds weird. Like, why two? You know, anyway this prover is supposedly very powerful. Why does he need another powerful friend?

So there was this idea, the following, that these two provers, they are like committing a crime. What's the crime? The crime is that they are trying to convince you of an incorrect theorem. And just like the police, the police is like the verifier, it's interrogating these provers. In order to check that their alibi holds up, they put them in separate rooms. They ask some questions from one, you know, potential criminal, and then they go and they ask and they compare questions to the other potential criminal, and this defines a model. What's the model? We have two provers. We have one verifier. The verifier can ask questions from each one depending on the question he asked the other, and the restriction on the two of them is they can't speak to each other.

That's a new definition of a proof system. We still want the fact that only correct statements should be convin- … there should be proofs only for correct statement, there shouldn't be proofs no matter what these two guys do for incorrect statement. But now we have an assumption, except it's not that factoring is hard but that these two guys are disjoint from each other. And of course I had some idea that it's not so bizarre, because we can think of an ID card, because I was thinking about Adi's motivation – that instead of having one ID card, you would have two of them and you put them into a bank machine. There were already bank machines at that point. Which might not sound interesting to you, but ATMs are also an invention that occurred during that time. [laughs]

Prof. Rosen: I'm not that young.

Prof. Goldwasser: You're not that young. [laughs] Okay. Neither one of us. In any case, so there are two cards, and you think about there's two cards, there's two provers, they're proving that they are Shafi. And the ATM is the verifier and it could make noise so they can't talk to each other, they can't see what questions are being asked. We had a patent on this.

Prof. Rosen: Oh really?

Prof. Goldwasser: Yeah.

Prof. Rosen: Okay, so I think maybe now maybe we can actually go down the line with this line of research and then I'll go back to the other area later.

Prof. Goldwasser: Okay, sure.

Prof. Rosen: And the chain of implications is very interesting I think, so maybe …

Prof. Goldwasser: Right, right. In any case, we had this model, the two provers. Why did we invent this model? Because it turned out that you could prove that every theorem that has a short statement has also a short proof, has also an interactive proof or a multi-prover interactive proof where these two guys, they have separate rooms and they're going to convince the verifier of the correctness of the statement without giving him the proof in zero knowledge, no assumptions. Okay, so there was a system. We did it for zero knowledge in order to remove the assumptions like factoring is hard.

Then there was a paper by I think Fortnow, Rompel, and Sipser where they showed that you don't … – what was it? – how many rounds you needed for this two-prover system. Then a whole bunch of results started to follow.

And then there was this incredible, incredible result by Noam Nisan, who was a postdoc at the time at MIT. What he showed was you can with a two-prover system prove the value of a permanent to a verifier. Now I don't want to get into the technical definition, but this is a very, very hard problem. It is extremely … It's beyond NP. And all of a sudden it seemed like … And additionally it's a complete problem for counting sharp-P class and it seems like the two provers were extremely powerful. And what followed after that is that using the techniques that Noam used, within sort of a whirlwind of results it has been shown that this class of interactive proofs with a single prover was as powerful as polynomial space. And then again, within months or weeks, it was shown that this class of two-prover interactive proofs was as powerful as non-deterministic exponential time. All of a sudden, these weird creatures that we've introduced with provers and verifiers and interactions and people locked in different rooms were sort of

grounded in the traditional complexity theory with classes like polynomial space and non-deterministic exponential time and equivalences were shown.

Prof. Rosen: And how did you feel at that time?

Prof. Goldwasser: What, the fact that all of a sudden … ?

Prof. Rosen: About yourself, your contribution.

Prof. Goldwasser: I thought it was … first of all, the mathematics was fantastic. It was really new mater- … It was arithmetization of polynomials, how to express languages. So the math was fascinating and I thought that …

Prof. Rosen: You were pleased?

Prof. Goldwasser: I was pleased. Yes, I was very pleased.

Prof. Rosen: Okay. Let's continue on that line and then we'll rewind back.

Prof. Goldwasser: Sure.

Prof. Rosen: So then you had the result and you went to DIMACS?

Prof. Goldwasser: Yeah, then I had a couple of years later, I think it was like 1990, I was in Princeton for a sabbatical and I think Joe Kilian gave a talk there about something about … I can't remember anymore. Some two-prover proof system in non-deterministic exponential time. And there was something about his talk that made me think that you could sort of simulate non-deterministic … you could do all non-deterministic exponential time in exponential time. [2:30:00] Which, like, you would show collapse of these deterministic and non-deterministic classes. And I told Muli Safra about that, who was actually my postdoc at the time I think, and he was also in Princeton.

We started talking about it and then it turned out that that would be true if – now it seems like a rabbit out of a hat – if some graph-theoretic problem was easy to approximate. The graph-theoretic problem is called the clique problem. It's like you have a graph and you would like to find a subset of the graph where all vertices have edges between them. It turned out that if you could approximate the size of the largest clique in a graph, then you could have showed that non-deterministic exponential time was equal to exponential time. Turning this on its head, it says that it's hard to approximate the size of the largest clique in a graph if non-deterministic exponential time is not equal to exponential time. Then when you sort of downsize this, you get essentially a result that says that it's hard to approximate clique if P is different than NP. So there's an NP-hardness result hiding in there.

Prof. Rosen: So you sort of started with complexity, went to cryptography, and came back?

Prof. Goldwasser: And came back, yeah. And this whole idea of using multi-prover interactive proofs, something that then morphed to something called probabilistically checkable proofs, PCPs, started with that work, and how to use that in order to prove hardness of approximation started with that work. That's become a complete field. That I'm very proud of.

Prof. Rosen: Rightfully so. So, okay. So now you want to continue a bit on this thread or go back to the other paper with the … ?

Prof. Goldwasser: So let me just say a few things about this. We've talked about interactive proofs, right? Single prover and verifier. We've talked about this multi-prover interactive proof. What is this probabilistically checkable proof? So far, everything was just very general, right? There are these two provers, there's a verifier, they exchange messages, at the end the verifier accepts the proof, doesn't accept the proof, there's some probability of error. But now we start quantifying things a bit. So you can talk about how much randomness is the verifier using? How many coins does it have to toss? You can talk about the length of the messages that are being sent. You can talk about how many questions are being asked and you can talk about the probability of error. And once you start quantifying this, it turns out that the value of these, these are parameters, and if you change these parameters, they can be sort of very tightly coupled to the problems that you can either approximate or non-approximate.

But let me say it in a different way. There's this third creature, which I mentioned, probabilistically checkable proof. What is that? There the idea is much easier to understand. In a sense, it doesn't require the stories of provers and verifiers and so forth, even though I love stories and I would never have got into any of this without stories. So probabilistically checkable proof, the idea is the following. Usually people think of proofs, mathematicians think a proof is a string that you can read in a book, right? It starts from statement one, statements follow, QED. Probabilistically checkable proof is a way to write a proof in such a way that you can actually … you don't have to read the entire proof. You can probe it at some locations, not in all of them, and you should think of it as if I'm choosing these locations at random, and make some check on those locations you've probed, some local checks, and if there is a mistake in the original proof, there's a very good chance you'll find a mistake in the local check.

So it's these proofs which are probabilistically checkable because you're sort of choosing the locations at random, and furthermore you have to read a lot less than reading the entire proof. Of course, you don't get certainty. You get probability of success. And now the kind of parameters that I talked about a minute ago come into play. How many places in the proof do you have to look at? What is the probability of error? What are the sizes of the questions and

answers? And these are parameters that, in the original paper that I had with Muli and then with Lovasz and Feige who joined … we joined forces, these parameters were improved subsequently by work by Arora and Safra and then by some well-known paper by Arora, Lund, Motwani, Szegedy, and Safra to be sort of optimal, where you really need just log *n* randomness and look at constant number of bits of the proof and you will catch a mistake if it exists.

Prof. Rosen: Szegedy and Sudan.

Prof. Goldwasser: What?

Prof. Rosen: Szegedy and Sudan.

Prof. Goldwasser: Szegedy and Sudan.

Prof. Rosen: Yeah. PCP.

Prof. Goldwasser: Yes.

Prof. Rosen: You describe PCPs and now you want to talk … let's rewind back to the late '80s to the second result you were alluding to.

Prof. Goldwasser: Right. That's a result with Ben-Or and Avi, and that's about how to do multi-party computation, the same problem I told you about with the different hospitals that want to compute let's say. It's a beautiful result which shows how to essentially turn this into algebraic problem where the data that you have is represented as essentially shares of a polynomial. This is something actually … it's called secret sharing that was invented by Adi Shamir, is how to take a piece of data and share it among *n* people so that only looking at some of the shares you have no idea what the data is, but if you have sufficient number of shares you can reconstruct it.

But Adi's secret sharing just was a way to share data. What we were asking is how do you compute on data? So now we have these three hospitals. Let's say each one of them has shared their data, secret-shared among all three. But that's not enough. They want to do a computation on it, like they want to do maybe some linear regression or they want to find out how many patients are there whose DNA is of a specific type and have had infections in the past and their blood test is in a certain range. So they want to do maybe set intersection or something like that. You can write any such function as essentially a sequence of operations on the data, which essentially looks like you can … I'm not going to explain how, but essentially looks like summing and multiplying.

What we realized is how you can take these secret shares which were essentially values of polynomials and compute with them. How can you add them and how can you multiply them where I only have my shares? I have the shares of your

data, I have shares of everybody else's data, and using these shares I can essentially compute a share of the sum of the data, a share of the product of the data. I can keep doing this iteratively and the end result is that essentially any program that we want to run on this data can be run in such a way that at the end I will only have a share of the result and I will have learned nothing about the data except for that share of the result. And since all of us have shares of the result, now we can reconstruct the result. That means that I knew my input, I'm going to know the result, and I can tell whatever is implied by knowing my input and the result and nothing else. And this is … It's important. [laughs] Yeah.

Prof. Rosen: Why is it important?

Prof. Goldwasser: Again, for lots and lots of application these days. If you want to connect it, if we kind of zoom to 2017, you know all the rave now is machine learning, right? Everybody's talking about these neural nets and logistic regression and how it is going to change our lives, for medical, for actual medicine, precision medicine, for targeting consumers, for making decisions on who to set on bail and so forth. But there is a question, and that is a lot of this is driven by the fact that we have tons and tons of data about people, and this data sometimes should not be shared. And it's held let's say by either individuals or by entities that even are bound by regulation not to share it. So how are you going to get them to share their data to be used let's say by machine learning algorithm in such a way that still respects the privacy of individuals?

The technique of multi-party computation is essential for that, because you may think of coming up with a machine learning algorithm, let's say in the training phase, taking the data, training on it and figuring out a model that can do predictions as a protocol which has access to data toward the end of coming up with a prediction algorithm, but not for seeing the data explicitly. And multi-party computation because of its generality can be used.

Now there's a difference here between theory and practice. On paper all is good. That is, we wrote papers and we proved theorems. But in order to use it in practice in a way that's efficient enough, you need to do a lot of optimization, you need to improve, you need to implement. Only time will tell if these methods will be used as they are or they will be modified, and hopefully not modified to such an extent that they will be insecure.

Prof. Rosen: Well, they are already being deployed in a commercial context.

Prof. Goldwasser: Yes.

Prof. Rosen: Okay, I'd like to switch gears for a moment now and go back to the personal. From the scientific to the personal. Maybe you can guide us through your experience from a personal perspective.

Prof. Goldwasser: Sure. So we were at MIT and there was this exciting time of being an assistant professor. Then all these results happened. And then I came to Israel and had that sabbatical, which had [2:40:00] more kind of interesting breakthroughs. And on a personal level, you know, I was getting older. I got married with a guy that I met in Israel and I had two children, Yonadav and Lior, and they are five and a half years apart. They are incredible, each one in his own way. And being a parent is different than being a scientist. It's all-consuming and the well-being of these children is everything. It becomes everything. And being able to balance that with being quite driven, having this job in MIT, and we haven't talked about that, but after I got married, I also decided to spend some of my time in Israel and I got a job in the Weizmann Institute, which was a wonderful place with wonderful colleagues. It is a wonderful place with wonderful colleagues. Incredible powerhouse.

But having children and having these sort of dual homes academically meant that we lived our life in a certain way where the kids spend … we all spend some few years in Israel, then a few years in Boston, and then in Israel and then in Boston. And it's true that a lot of academics go on sabbaticals, they go on leaves, the children travel all over the world. In our case, it was maybe more planned. So I think a lot of academics, every four years they go someplace. But we really knew that every 3-4 years we'd get up and go. The good side was that we always went to the same place and the kids had the same schools. But the fact that it was kind of a predestined departure gave an alternative structure to our life which I think is unique. And there's probably a lot of people watching this, if anybody's watching it, know that being a parent is associated with a lot of responsibility and a lot of guilt. And I have plenty of it. But you know what, they came out pretty good. [laughs]

Prof. Rosen: But in hindsight, would you do … ?

Prof. Goldwasser: "Would you do it all over again?" That's a great question, right? I think I would do my scientific career all over again in the same way. Would I have done this back-and-forth thing? I don't think hindsight is something that we can actually act on, is it? And therefore it's pointless …

Prof. Rosen: Definitely not. Okay.

Prof. Goldwasser: At any point in time, it didn't seem like there was any choice except to do what we did.

Prof. Rosen: No point in regretting it?

Prof. Goldwasser: It's just it was so compelling. You know, I think everything in my life has always been sort of unavoidable in the sense that I was so compelled to do it and I couldn't see it from the outside, I could only see it from the inside.

Prof. Rosen: Do you have other examples of this phenomenon?

Prof. Goldwasser: Of seeing things only from the inside?

Prof. Rosen: Of being compelled to do something and …

Prof. Goldwasser: Yeah. I guess I am about to embark on a new adventure. As I told you, I've been at MIT, I've been at Weizmann for many years. I've done this back and forth, I've had my children, I've had my career, I've had my marriage life. I've taken care of my parents for many years. All these things are things one is compelled to do. And in the last year I've decided to go back to Berkeley to head an institute for theoretical computer science, or foundations of computer science, and I think that I've kind of experienced the same compelling … "Compellment"? No. I've experienced the same type of … I've experienced the same kind of internal drive or internal push toward a decision which may look in hindsight a bit surprising, because I have a fabulous job at MIT and a fabulous job at Weizmann. And I already have a full life, and all of a sudden there's a third thing that's thrown into the wrench, but I feel compelled to do it and …

Prof. Rosen: You long to recreate the Berkeley days?

Prof. Goldwasser: Maybe. Maybe. You know those green hills and that beautiful …

Prof. Rosen: Blue sky?

Prof. Goldwasser: … blue sky. [laughs] There's something to that.

Prof. Rosen: Okay. Is there something you want to add in this context?

Prof. Goldwasser: No. I'm looking forward to a new adventure.

Prof. Rosen: You were talking about this duality, Weizmann, MIT, back and forth. Would you be able to compare the two places in terms of culture, in terms of differences?

Prof. Goldwasser: Yes, yes. MIT is very intense. There's a lot of people. A lot of graduate students. I have right now eight graduate students at MIT and a lot of postdocs and colleagues. And there's continuous seminars and meetings, and you really feel like you're in the midst of it. And Weizmann has fantastic faculty members, very, very good graduate students, but fewer. And the doors are sometimes more closed than open, even though it's changed I think in the last years. So there's more time to think, but there's less intensity, and I think that they're very different that way. And it's hard to tell what's right for which person. For me, I know that both would have been beneficial, but in a different way. So I think that after a few years in Weizmann, I was very eager to go back to MIT, and

after a few years at MIT, I was very eager to rest a little bit and just kind of be able to think. And now I have no idea what it's going to be like at Berkeley. Maybe I could both think and be intense, and maybe I'll just [laughs] have a completely new experience.

Prof. Rosen: And has it always been so intense at MIT invariably through the years?

Prof. Goldwasser: Yeah, I think so. I mean there are years where sort of cryptography specifically has gone through a lot of revolutions. There was the time that I described in the '80s and in the '90s. Then there was a time that was quieter. There was this beginning of lattice-based cryptography which I was also a little bit of a pioneer at, and there were fewer people who were working on it because it's harder material. But now we are again in the midst of a big revolution, which is talking about these new methods of encryption where not only you encrypt but you can actually compute on encryption, called homomorphic encryption, and there's things called program obfuscation. And there's many, many people in the field and they are often working on similar problems, so there's a lot of conflicts in the sense that people are submitting the same results to the conference and then they merge them or they unmerge them. It's a very different pace.

Prof. Rosen: And that's something you mentioned before that you feel uncomfortable with, working on the same problem that everybody's working on.

Prof. Goldwasser: I'm not sure I can really compete when everybody's working on the same problem. I think my strength is more at sort of defining the problems, maybe defining, sort of coming up with an original idea or method. Proving original … the first results. When it already becomes so well known that a lot of people are working on it, I don't think that I am so fast and so technically alert that I could derive the pleasure or even derive the outcome.

Prof. Rosen: Okay. Now I'd like to ask you about some retrospective about advising students throughout the years.

Prof. Goldwasser: Sure.

Prof. Rosen: Because you'd had many great students, well known, very successful, and in several ways, in several generations.

Prof. Goldwasser: That's right.

Prof. Rosen: So …

Prof. Goldwasser: Alright. First of all, I have had incredible students, and these students, I am thankful for that every day. Early in my career I worked with my

colleagues. You know, I worked with Silvio and Oded and Avi and others, so I'd never really wrote papers with my students. But now I do. But in any case, invariably first the students were really more doing their own thing and I was advising them in the sense that they would tell me about their stuff, and sometimes questions came from me, sometimes questions came from them. Now it's more that I'm in an advisory role, that most of the questions come from me, but the students do a lot of the work. I think that my advising style must have changed because it became much more working together with the students than it was before.

I'm always in awe at the fact that there's a new student and there's a new talent and that they really make something out of nothing. Not in the sense that they are nothing. In the sense that they come up with new ideas and new questions, and where does it come from? That's the incredible thing of working in university. There's this young generation one after the other, and they are so excited about what they do and they are remarkable. So that's really a gift of being able to be in university.

Prof. Rosen: Okay. Can you mention different styles of students, of researchers that you encountered? Different characters?

Prof. Goldwasser: Different characters. I've met lots of characters. [laughs] I remember Joe Kilian was really into limericks and a great sense of humor and a very creative, unusual researcher. Then there are people who are very like technically extremely sharp, right? I mean so was Joe, like Johan. [2:50:00] And I'm mentioning the people in the beginning, because at my advanced age [laughs] it's easy to remember the past rather than the present. No, but I've had amazing students really all along. Some of my students are faculty members at Weizmann where we're sitting right now, like Zvika Brakerski and Guy Rothblum, who've both done amazing things. Then some of my students are faculty members at MIT like Vinod Vaikuntanathan. Then there's Yael Kalai. And I have students all over Israel, like Yishay Mansour and Adi Akavia and many others all over the world.

Prof. Rosen: So now we can leisurely talk about the property testing and delegation?

Prof. Goldwasser: Sure. Okay, so property testing.

Prof. Rosen: How did it all start?

Prof. Goldwasser: How did it all start? I actually think that my first thoughts in the direction of property testing come again to a talk that I attended in Hebrew University of Michael Kearns actually where he talked about learning. He had some model of statistical query learning. In any case, and then I drove back with him to Tel Aviv and we had some conversation in the car that made me start

thinking about the question of not learning where you are trying to essentially … you have examples and you're trying to predict a label of a future example, but more being able to tell a property of whether the examples you are seeing belong to one distribution or another distribution.

Or another way to say about it … What do I mean by examples? It's too generic. Let's say that you have a function and you can't look at the function table. You actually don't have a description of the function, but you can query the function in different places. And what you would like to find out is a property of this function. So what could be an example of a function? An example of function could be let's say there's a graph and I actually can't look at the whole graph because the graph might be extremely large, but what I have is I could apply a function to two vertices and the function will say one if there's an edge between them and zero otherwise.

So that's a description of the graph. It says a function. So there's sort of an indirect description. Now I'd like to ask questions about this graph. Is this graph three-colorable? Is this graph connected? Can this graph be partitioned into two sets of vertices that there's only edges going between the sets and not between vertices within the two sets? It's called a bipartite graph. So that's a property. And obviously some of these questions you have to look at the entire graph. You have to sort of ask the function, the entire function table for every pair of vertices, what the edge is and then solve the problem.

Then property testing though says, "You know what, let's relax the question, because we really cannot write down the whole graph, we cannot query the function in all places. We'd like to tell whether the graph that's being described by this function which I can sort of query is close to a graph that has that property." So if we think … Let's look at a specific graph property that's say connected. This graph that the function is describing, it's either connected or it's far from being connected. What do I mean by far being connected? It means that if you look at the closest graph to it by removing edges or adding edges, let's say it's epsilon apart. You have to add epsilon or subtract epsilon edges. And I'm talking about epsilon rather than … because I'm normalizing here. So there's a fraction of edges that you have to insert or delete, and I'd like to tell which is the case. Is it a connected graph or is it far from a connected graph? And I'd like to do that by querying the function in very few places.

So for the layman, let's think of it this way. We are not living in the age of dinosaurs anymore, right? We find bones of dinosaurs. Can we just by looking at bones of dinosaurs tell whether the entire dinosaurs was a tyrannosaurus? Was it a meat-eater or herbivore? Apparently people make conjectures based on very little data. So the question here is if I can only look at very little places in the graph, either given or I can query the graph at places of my choice, can I tell something about the graph more globally, like being connected or being far from connected?

This is the way I like to describe property testing, and that's a field that … a paper together with Oded Goldreich and Dana Ron. We wrote on testing properties of graphs and more generally testing properties of natural structures. You know, graphs as a natural structure or other functions are possible too, not just to described graphs. And we would like to find out whether a function let's say is monotone and we can't write down the whole function table. We can just query the function in a few places. Can you tell if it's monotone or far from monotone? This is a field that's become a whole field. I mean that paper I think was fairly influential.

And then you asked me about delegation?

Prof. Rosen: And lattices, if you want to mention some more about lattices.

Prof. Goldwasser: You're going to mix this in I assume?

Prof. Rosen: I'm not going to do anything, but maybe, yeah, with their help.

Prof. Goldwasser: Yeah. I think I'll talk about delegation.

Prof. Rosen: Okay.

Prof. Goldwasser: So time moves on and people start talking about different models of computation like cloud computing. And the idea of cloud computing is that there are these computers out there and I'm a client, and I'd like to use the computers and they will do all the computation for me and then give me the results. So the clear question is how do I know they are even computing it correctly? I am delegating my computation to an outside computer. I want to get some proof that the result has been correctly computed. We call this a delegation problem, and that's a problem that is a little bit similar to interactive proofs because this computer proves a statement to me. The statement is that it did the computation correctly. That's been a problem that I've been very interested in.

And the delegation paradigm isn't just delegating computation, but you can think about it in other contexts, like you want to delegate in the context of error-correcting codes. Let's say I want to code a message in such a way that even if there's noise on the line, you can detect it. Then there's the question of how much work you have to invest in order to encode and how much work do you have to invest to decode, and you can talk about delegating work of the encoder to the decoder or vice versa. So this whole delegation paradigm is something that I've been interested in in the last, I don't know,15 years already. And that's been fascinating. This is work with my students Yael Kalai and Guy Rothblum. So that's something that I'm still interested in. I think that this delegation paradigm is very powerful in today's sort of modern computational world.

And you asked about lattices. As I mentioned, the theory of lattices has become the basis in hard problems on lattices. Like if you define some sort of integer lattice via basis, find the short vector in the lattice has become sort of the … this theory and these hard problems have become the basis of what we call post-quantum cryptography. And implementing sort of essentially cryptographic primitive based on these type of problems is a fascinating field which I've been involved in.

Prof. Rosen: And you were very early on.

Prof. Goldwasser: Yeah. This was work with Oded Goldreich, where we sort of asked this question of interactive proofs to show that a shortest vector in a lattice is not so short and we introduced some new methods in this field.

Prof. Rosen: You actually, yeah, introduced a method to show that it's going to be unlike … it's unlikely to be as hard as other approximations.

Prof. Goldwasser: Yeah. But in any case, the method is more important than actually the result because the method is essentially what underlines a lot of proofs of security in modern cryptographic systems that are based on this post-quantum cryptography.

And I want to mention actually one more student, Daniele Micciancio, who was one of my students, which I love very much. He started working on logic actually with Albert Meyer, his master's, then he came and worked with me about digital signatures. And for his exam … There are these exams at MIT which don't exist anymore where you're supposed to give a student a few papers and then they are supposed to read it and do some original contribution within three weeks. So I gave him some papers on lattices and he came up with some beautiful new result proving the hardness of approximation of shortest vector in a lattice, and that became his field of research. I feel privileged to have suggested the problem to him, or the papers to him. I think he's one of the sort of guiding lights in the field of lattice-based cryptography.

Prof. Rosen: Okay. You want to mention something more about students?

Prof. Goldwasser: I think that I have a new crop of students which are wonderful, and they're doing … Today it's actually interesting. A lot of the students are not only interested in sort of the science, but they're actually interested also into impact on society. So this is sort of a modern wave. I mean as you see people, you know there is this generation that's just interested in going to startups and the generation that's just interested in doing complexity theory and then doing cryptography. And the new generation that I have at least, they're very interested in the impact of the methods on today's world. And when I say impact, [3:00:00] I don't mean just implementing systems that are run

efficiently, but really questions of like how is this going to change the world from a society point of view?

Prof. Rosen: So for them, the application might be more of a guideline?

Prof. Goldwasser: The application might be more of a guideline but it's not an application that is necessarily only having to do with utility. But it actually also has to do with doing good. I mean privacy anyway is doing good in my book, but it's beyond that.

Prof. Rosen: And what's your take on privacy, whether it's doing good, whether it helps?

Prof. Goldwasser: Of course it's doing good. I mean it's you know the usual line that I think they attribute to Judge Brandeis, but I think it was Brandeis and another lawyer, that they were in a law firm together and this is after the original cameras were invented, the kind of cameras, portable cameras that you could take out of the camera shop. And they wrote this paper about "What about the right to be left alone?" You know, it's very nice that you can take photographs, but now I could be taken a photograph without my permission. Now imagine where we are at. Right? Everything we do on our iPhone, every Google query we make, every email we send is being recorded by these big giant companies and they are deriving conclusions from it, like giving us advertising for us. So the right to be left alone is something nobody imagines anymore, you know with all these sensors and the cameras. It really alters our reality and I think we need to think about it.

Prof. Rosen: And you don't think it's too late by now to do anything about it?

Prof. Goldwasser: You know, it's just like talking about the environment, right? So with the envir- … we have a lot of pollution, but somehow it's self-regulating. Not as well as it should be, but there are climate agreements and people don't sell the kind of cars they used to. There's emission controls. So my feeling is that every revolution has at some point people realize that there are some things to fix. And I don't see why the lack of privacy is not going to be the same, because the methods exist. And we can develop more methods. But people have to be aware, people have to kind of pull back, people have to implement these methods on top of the existing ability to spy or to have sensors and …

Prof. Rosen: And what about the negative implications of the ability to encrypt data and hide it from others?

Prof. Goldwasser: The negative implications?

Prof. Rosen: Yes.

Prof. Goldwasser: Yeah. I guess the negative implications is that we could go dark, right? This idea that now that the encryption methods are being developed and they're so strong and they're so well known, that we won't be able to pursue criminals, right? So being able to read messages, being able to wiretap, being able to listen to digital communication is a police tool. It is a national security tool. We all know there's more and more threats.

So by enabling this encryption for the public, you are in a sense making it more difficult for law enforcement to behave. I buy it, but it's a very thin line, right? On one hand, privacy has so many good outcomes. It's enabled electronic commerce. It's enabled a use of remote computers for delegating computation. It's going to enable doing machine learning on data while keeping it private. On the other hand, there are these criminals who should be caught and we should enable law enforcement to catch them.

How do you reconcile the two? One opinion is that you just say, "Well, tough. Let the law enforcement figure out other methods to catch criminals and don't give up on privacy." And another point of view, which is the other extreme, is let the law enforcement have all the keys to all the encryption algorithms out there. And maybe there's a third sort of economic model where you sort of think of cost-benefit analysis and you're able to trade it off, so you can sort of trade off privacy in policing. I don't think people have looked at it, but just again, if we go back to the example of environmental science, there is sort of a cost-benefit analysis of putting regulations, and there are resources that are renewable, resources that are not renewable, and there's measures. So this is not really my expertise, but I can imagine a world where that kind of theory is developed also with respect to privacy.

Prof. Rosen: What about the future?

Prof. Goldwasser: That's the thing about the future, you don't know do you? As we say in Hebrew, "Yehie Tov" (יהיה טוב) *[Trans: all will be well].* [laughs] No, you're asking about the scientific future. I …

Prof. Rosen: Not necessarily.

Prof. Goldwasser: Not necessarily. The future is that I'd love to continue doing research. I love interacting with young people, with postdocs, with graduate students. I'm still inventing new questions. We haven't talked about them, but that might be in another interview. And I still get excited from new questions and new answers. I'm looking at what has happened to cryptography. It's kind of amazing in terms of the number of people and the impact and the excitement, so this is sort of a future which is inevitable. It's not sort of … There's no question that cryptography has a future. And personally I hope to do more. I hope the field will do more. I'm very optimistic.

Prof. Rosen: Where do you see yourself five years from now?

Prof. Goldwasser: You know what, I think that's the one question I can't answer. [laughs] I don't know.

Prof. Rosen: In terms of aspirations, just … ?

Prof. Goldwasser: I want to keep on working. I want to keep on creating. I want to have ideas. I want to have impact, and the kind of impact that I'm talking about now is also impact as let's say the director of the Simons Institute or someone who directs … someone who has some influence about where the field is going in the sense of what's important and what's not important. I think that I've had a good hunch and I feel I have an intuition to serve me and also a lot of experience. So if I have made impact in the next five years both in terms of research and in terms of leadership, if my kids do well and they're happy, then I will be very happy in five years.

Prof. Rosen: Okay. Thank you very much, Shafi.

Prof. Goldwasser: Okay. Thank you.

[3:07:05]
[End of Recording]