UNIVERSITY OF AMSTERDAM

UvA-DARE (Digital Academic Repository)

A cryptographic view on computer science

Schaffner, C.

Publication date
2022
Document Version
Final published version
License
CC BY-NC

Link to publication

Citation for published version (APA):
Schaffner, C. (2022). *A cryptographic view on computer science*.

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE is a service provided by the library of the University of Amsterdam (https://dare.uva.nl)

Download date:31 Aug 2023

A Cryptographic View on Computer Science

Prof. dr. Christian Schaffner*

University of Amsterdam, The Netherlands

Inaugural lecture delivered on Friday, 30 September 2022

Abstract

Cryptography is a fascinating research field with a long and intriguing history. Modern cryptography is ubiquitous in today's digital society, as it can provide security in any situation where parties do not trust each other. In my inaugural lecture as *Professor of Theoretical Computer Science, with special attention to Quantum Computing* at the Faculty of Science, I demonstrate how cryptographic concepts are naturally linked to fundamental questions in theoretical computer science; for example in complexity theory (how fast can a computer solve certain problems?), information theory (how much information can be sent over a bad connection?), discrete mathematics (e.g. how many prime numbers are there?) and quantum computing (what are the power and limitations of this new kind of computer?). I sketch my vision of how to build a research group, education infrastructure and ecosystem to address these fundamental problems.

Recording and Supplementary Material

On my academic homepage at `https://staff.science.uva.nl/c.schaffner/oratie/`, I provide a link to the recording of my inaugural lecture, which contains all the visuals and audio. I highly recommend watching the recording rather than reading the following plain text of my inaugural lecture. At the same link, you can also download my presentation slides and some cryptographic entertainment material we produced for the attending children.

A cryptographic view on Theoretical Computer Science

Mevrouw de rector magnificus, meneer de decaan, dear colleagues, dear friends and family,

There's a famous legend about the origin of chess that goes like this:[1]

[slide 2] When the inventor of the game showed it to the emperor of India, the emperor was so impressed by the new game, that he said to the man: *"Name your reward!"* The man responded: *"Oh emperor, my wishes are simple. I only wish for this. Give me one grain of rice for the first square of the chessboard, two grains for the next square, four for the next, eight for the next and so on for all 64 squares, with each square having double the number of*

*c.schaffner@uva.nl

[1] from `https://www.dr-mikes-math-games-for-kids.com/rice-and-chessboard.html`

grains as the square before." The emperor agreed, amazed that the man had asked for such a small reward — or so he thought. After a week, his treasurer came back and informed him that the reward would add up to an astronomical sum, far greater than all the rice that could conceivably be produced in many many centuries!

I'm sure some of you have heard this story which illustrates how quickly numbers grow if we keep doubling them, it illustrates the craziness of exponential growth.

[slide 3] Arjan van de Meij, a Dutch member of the maker scene, has illustrated this growth here on this physical chess board [2], where these piles of rice reach the height of Mount Everest in the fourth row, then reach to the moon, to the sun, and eventually beyond our own solar system. Impressive, isn't it?

In the coming 45 minutes, I would like to give you an idea of the kind of work that I do.

[slide 4] Concretely, I will offer you *a cryptographic view on Computer Science*. I would like to convince you of two things. First, that modern cryptography is a fascinating field of research. Second, that it is naturally linked with fundamental questions in Theoretical Computer Science.

[slide 5] You might wonder what Theoretical Computer Science (TCS) even means or what it is. For me, it forms a sweet home of applied mathematics, spanning a range of different disciplines, some of them listed here, and you will get a glimpse of them through the lens of cryptography.

Cryptography

So, let us begin: I have been fascinated by cryptography for as long as I can remember. There's some magic about keeping information secret from others, and it is something that humankind has been doing for thousands of years already.

[slide 6] As you can see on this timescale, reaching all the way back to the ancient Greeks who have used a *skytale*, a piece of leather wrapped around a piece of wood to write their message on. You can imagine that if you unwrap the leather, the order of the letters will be scrambled, and only if you possess a piece of wood of the same diameter you can reconstruct the message. Through the history of cryptography, we encounter quite a few famous names like Caesar, or Vigenère of which you might have heard of.

[slide 7] Zooming into the last 200 years, we encounter people like the Dutchman August Kerckhoffs who put forward a couple of cryptographic principles, the most famous one states that *"a cryptographic system should be secure even if everything but the key is known to the adversary"*.

Moving on in time, we encounter the German enigma machine and the story of Alan Turing and the allied efforts to breaking this machine. We encounter Claude Shannon, the father of information theory and inventor of the term *bit*, before we enter the age of modern cryptography, where [slide 8] cryptography is simply everywhere around us, as it concerns all settings where people do not trust each other. Examples are secure communication on the internet, military contexts, opening cars, access control to building, and of course, our computers and smartphones are full of cryptographic functionalities.

[2] `https://www.instructables.com/Chess-Board-Full-of-Rice-Exponential-Growth/`

[slide 9] But how can we establish secure channels? An aifachi Möglichkeit isch, dass i relativ schnell Schwizertütsch reda. In dem Fall verschtönd plötzlich dia maischta Lüt in dem Saal nüma was i eigentlich säga. Dass bütet miar au dia kurzi Glägaheit alli Gäscht us dr Schwiz herzlich zbegrüassa do und mi zbedanka, dass iar bis do uf Amschterdam kho sind. Entschuldigung, wenn iar dr Rescht vu minara Red nit so guat könnt verstoh.

Ik zou ook Nederlands kunnen praten, dat veel meer mensen hier in de zaal kunnen verstaan, maar waarschijnlijk zijn er niet zo heel veel, die zowel dit als ook mijn laatste paar zinnen goed konden volgen.

What I just did was establishing channels to certain people in this room that are able to understand these other languages. This is an example of *code talkers* that have actually been used in a military context, the most famous example probably being the Navajo native people that have helped communicate the US and the allies in the second world war by talking in their native language.

Is "code talking" secure? It depends on how many people can understand the language.

Perfectly Secure Encryption

Let me show you a much more secure way of encryption.

[slide 10] In order to do so, I quickly need to teach you how to add and subtract letters and numbers from each other. Have a look at these circles. We identify all letters with a number from 0 to 25. Let me show with this example how to add the number 4 to the letter `D`. We look up `D` on the inner circle, which is 3, so $3 + 4 = 7$ which corresponds to the letter `H`, which is `D` shifted forward by 4 positions.

In the second example we add 10 to `T`, so $19+10 = 29$ which is bigger than 25, but we simply keep counting, and end up at 3 which is `D`. In mathematical terms we call this wrap-around *working modulo 26*.

Similarly with subtraction: Subtracting 10 from `D` is $3 - 10 = -7$ but that is the same as 19 modulo 26, which brings us back to `T`. That is not so surprising as we started off at `T`, added 10 and subtracted 10 again.

So, we have been practicing this a little bit at home, and it turns out that my daughters Elin and Nova have become pretty good establishing a secure channel among them. Let me invite them to the stage to show you how. They are using these cipher wheels that we have distributed among the kids here in the audience.

So, this morning they have agreed on a secret key, they have picked four numbers between 0 and 25 as their secret key, that nobody else knows. For the sake of this example here, say the key is $k = 10, 13, 22, 22$. Now, Elin will play the role of Alice in this cryptographic protocol. A protocol is simply a recipe describing the steps that the players carry out.

Alice/Elin takes the four-letter message she would like to send to Bob, and adds the letters of the key to it, resulting in a ciphertext c. For example, if she wants to send the message `TEST`, using the key $10, 13, 22, 22$, that results in ciphertext $c =$ `DROP` which is sent over the line to Bob. Then, Bob/Nova can simply subtract the key again from the ciphertext c, and learn the message that Elin has sent to her.

[slide 12] Of course, in reality, we don't know what key or message they are using.

I see Alice smiling, so I think she is ready to send the ciphertext to Bob now. Ciphertext is `DROP`, hmm, conveniently exactly the same as in my example on the slide, OK. The ciphertext has been received, and Bob can now compute the message by subtracting the key.

Let's see if we can eavesdrop into their conversation. We have learned the cipher text c, but we don't know the key they had agreed upon beforehand. So given that ciphertext, could it be that their message was `TEST`? Yes, that's obviously possible, if the key was $10, 13, 22, 22$, as on the previous slide.

OK, is it possible that their message was actually `DROP`, the same as the ciphertext? (pause) Yes, that is a possibility, namely if their key happened to be $0, 0, 0, 0$.

Hmm, given that $c =$ `DROP`, could it be that their message was actually `NICE`? Yes, that is possible as well, as this key on the slide maps this message to the ciphertext `DROP`.

In fact, any message is possible from our (eavesdropper)'s point of view. So, in fact, that is a perfectly secure encryption system!

I see Bob smiling now, so she has learned the message that Alice has sent, but even with all the computation power in the world, we will not be able to learn a tiny bit of information about the message they have exchanged.

So, dear kids, this is a perfectly secure way of communicating with each other without your parents (or teacher) learning what you are saying.

In practice, it turns out that this so-called *one-time pad scheme* has some severe drawbacks.

First: The key has to be as long as the message, and it can only be used once. That is really not very convenient, as we would like to have short keys but want to encrypt long messages.

Furthermore, the keys need to be pre-agreed, which works well in the family setting at home where you see each other regularly, but what if I want to communicate with somebody with who I have not shared a key with previously?

Amazingly, I will be able to show you how to do that as well! This is one of the little wonders of modern cryptography. In order to understand how it works, we need to learn a little bit more (discrete) mathematics.

Diffie-Hellman Key Exchange

[slide 13] In this little example, we will repeatedly multiply 3 with itself, but don't worry, our numbers won't explode like in the chess story, as we are working modulo 7, so all numbers stay below that threshold. So first we have $3^0 = 1$, then $3^1 = 3$, and $3^2 = 3 \times 3 = 9$, and we work modulo 7, so 9 is equal to 2. Then we continue multiplying by 3, giving 6, then $18 = 4$, then $12 = 5$, then 15 which is again 1, as we close the cycle.

There is an easy operation, namely multiplying 3 with itself, and a hard operation, namely given an element of the group, telling how many times you have to multiply 3 with itself to get there.

Let's run the Diffie-Hellman protocol! Let's make it a bit more interesting: instead of modulo the prime number 7, we calculate modulo a bigger prime $p = 131071$ instead. I will pick a random number a between 0 and 131070 and raise 3 to that power, all modulo 131071, resulting in 278. Any mathematically inclined volunteer in the audience who wants to run the protocol with me?

My intended communication partner over there picks his own b, raises 3 to this power and shares the result with us: 23115. Finally, we can both compute a shared secret key. I take his number 23115 and raise it to my secret exponent a, and he takes my 278 and raises it to the power b. It's easy to verify that we both end up with $3^{a \cdot b}$, so the protocol is correct, as it works for us two who behave honestly.

Is it also secure? Putting ourselves again in the shoes of the eavesdropper, we learn the numbers C, D and we know that these are some unknown powers of 3 modulo 131071, but we cannot compute a, b, and k. Remember that it is easy to compute powers of 3, but not to figure out what the power is given the result.

From this example, we can draw a couple of theoretical computer science lessons:
Namely, the crucial difference whether certain tasks can be done on a computer *efficiently* (i.e. in a polynomial number of steps) or in *exponential* time. In this Diffie-Hellman Key Exchange protocol, the honest player needs to compute large powers of 3.

[slide 15] Consider the example of computing 3^{128}. Doing these exponentiations in the naïve way would still take a long time, namely 128 multiplications. Luckily, there is a more clever way which provides a nice shortcut. The crucial observation is that instead of doing all these individual multiplications, we could repeatedly square the number instead! In this way, we get to the result with only 8 multiplications. For large numbers, like in the Diffie-Hellman protocol, this will make a huge difference!

[slide 16] This shortcut is the crucial difference why the Diffie-Hellman protocol is secure. It's all about *scaling*. The honest parties can perform their actions efficiently (in polynomial time), but the attacker or eavesdropper is left with the naïve strategy of basically trying all possible a's in order to figure out the private values of one of the players. This brute-force search takes exponential time compared to the honest players.

In theoretical computer science, *it is all about scaling*. If we have identified this type of gap, we can run our protocol with large enough parameters that attacking it will become totally infeasible while honest players can still perform the protocol.

This is the wonder of public-key cryptography. Even though all of you have heard our conversation, you cannot learn the secret on which we agreed, so we can follow up with a conversation that is completely private to us. Isn't it absolutely amazing? This technique is at the core of what every one of us uses every day to connect securely to internet websites.

And if this was the end, we would all live happily ever after in our sweet Theoretical Computer Science land...

Enter: the Quantum Computer!

[slide 17] An entirely new type of computer which sounds a bit like magic if hear about it for the first time. Instead of classical bits that are 0 and 1, quantum computers use quantum bits (or qubits) that can be 0 and 1 at the same time, we call this a *superposition* of 0 and 1. One qubit can be in a superposition of 2 states, but 2 qubits can be in a superposition of 4 states, and 3 qubits in a superposition of 8 states, and you know how that goes with exponential growth, just 300 qubits can already be in a superposition of 2^{300} states which is more than the number of atoms in the universe. So, it's tempting to think that a quantum computer can do this many classical computations at the same time. This is kind of true, but the problem is that at the end of the computation, you must perform a measurement which collapses the outcome to a single classical outcome.

Therefore, the art of programming a quantum computer consists of exploiting another crucial ingredient of the quantum computer, namely *interference*.

[slide 18] You are all familiar with the interference of sound waves that travel through the air. A composer tries to create a beautiful interference of these ways.

[sound] Quite similarly, qubits in superposition can interfere with each other, and a quantum programmer tries to ensure useful interference of these states, so that only the result you want to obtain remains when you measure the state.

It is the core question of our research center QuSoft to investigate what the capabilities and limitation of this new type of computer are.

[slide 19] One thing we know due to a breakthrough result by Peter Shor in 1994 is that large enough quantum computers will be able to efficiently factor large numbers and to take discrete logarithms.

In other words, they will break exactly the Diffie-Hellman key exchange protocol (and other public-key cryptography) that currently protects our internet traffic! I agree with the generally believe opinion that the effects of such an attack would be quite severe, with many digital services not being available anymore. So, we want to definitely avoid this scenario.

So how long will it take before these quantum computers are powerful enough to break the current public-key cryptography? The honest answer is: we don't know, most likely at least 10 years. However, for some type of data like state secret or medical data, there exist laws on how long they need to be kept secure, and that can easily be longer than 10 years. So, even though this thread seems to be far away in the future, it might already be too late today, as we know that encrypted traffic is stored on a large scale, and they will simply be able to decrypt in 10 years from now when the quantum computer becomes available! Hence, there is some urgency to replace the current public-key cryptographic systems with new ones that (hopefully) remain secure against future quantum attackers.

Concretely, this field of *post-quantum cryptography* is one of the research areas that I have actively contributed to over the last few years, also with the help of my PhD students Jan and Jana, as well as many other people at CWI and at QuSoft who hare involved in this process.

[slide 20] Besides this somewhat negative view on the future impact of quantum technology, we also have good hope that quantum technology will be of great benefit to society! Maybe the most promising application is to use these programmable quantum computers to simulate other quantum systems that occur in nature, in order to better understand physical processes,

such as the fixation of nitrogen, or photosynthesis in plants.

[slide 21] From a cryptographic point of view, quantum technology will also offer new possibilities. A particular feature of quantum information is that an unknown quantum state cannot be perfectly copied, which is very different from classical (non-quantum) information, which can easily be copied. This no-cloning property can indeed be exploited to build new cryptographic methods that are not possible with classical cryptography. Furthermore, in the farther future, many parties might hold quantum information which they would like to compute on. However, quantum computers might only be available in special facilities. Hence, we would like to build a *quantum cloud* where one can secure delegate a quantum computation on your private data to a remote location, without revealing to the quantum server what you actually want to compute. This type of quantum cryptography is another field of research to which I have actively contributed over the last year, for example in collaboration with my IvI colleague Florian Speelman and my former PhD student and now Postdoc Yfke Dulek. My plan is to continue to do so.

[slide 22] So, I hope I have convinced you that modern cryptography is an exciting field of research full of surprises, and I have given you a peak through the lens of cryptography into our "sweet home" of theoretical computer science, illustrating some of the fundamental links between cryptography and various disciplines in TCS.

Vision on Research, Education and Knowledge Transfer

In the remainder of my lecture, I would like to explain to you my vision for the future in the area of research, education and knowledge transfer.

I have already sketched to you the "tip of the iceberg" of the kind of cryptographic problems that I expect to tackle, and how they relate to fundamental problems in theoretical computer science.

[slide 23] Since my start as group leader of the *Theory of Computer Science* group at the Informatics Institute at the end of last year, I have been involved in two major hiring rounds, and I am very happy to tell you that I was able to find two very promising young researchers with whom I will be building the new theory group. The first one is Nicolas Resch who is an expert in (classical) information theory and error-correcting codes. Nic is originally from Canada, did his PhD in the US and was a Postdoc in the CWI crypto group until recently. He will be expanding the group's expertise on the classical (non-quantum) research topics.

The second one is John van de Wetering who did his PhD in Nijmegen and is currently a postdoc in Oxford. John's research lies in the intersection of mathematics, physics and computer science, as he is an expert on ZX calculus, which can be used to manipulate and optimize quantum circuits. He brings in new complimentary expertise to the quantum research community of QuSoft.

Of course, I will continue to do my own *research*, with a couple of PhD students starting hopefully next year, and with a special attention on figuring out what the consequences for cryptography and for society will be if quantum technology becomes available in the future. I also have good hope that these new people will increase the diversity of our group.

[slide 24] The other important aspect of academic life is *education*, and here I would like to mention the fourth permanent member of our group, Steven de Rooij. Steven's job is almost exclusively focused on teaching, and he is currently teaching many of the theory courses in the BSc informatics program. Together with him, the other group members and I will try to

strengthen the theoretical aspects of the computer science curriculum both in the bachelor and master in the coming years.

Another teaching-related project that I'm particularly excited about is the setup of an entirely new Master program in *Quantum Computer Science*. For a scientist, it is quite rare to get the chance to design from scratch a whole new master program in your particular area of research. Together with my colleagues Paola Grosso and Kareljan Schoutens as well as Michael Walter, we have taken the first steps for setting up such a new program. After Michael's departure to Germany, John will be taking on the role of *scientific leader* of this project. The current planning is that the first cohort of students will start this program in Fall 2024. We are aiming at mathematically skilled students and hope to create a pipeline of graduates who will be able to continue to do academic research as PhD students, or to take on a job in industry.

When taking on such a new role as professor, and thinking about a vision and mission for the future, I naturally pondered the question of *impact [that I had or will have] on the (academic) world*, and in this context, I came to the conclusion that for me personally, my teaching-related activities might have more impact than writing research articles about fundamental questions in theoretical computer science. I also believe that this stream of highly educated students will be the "gold mine" of the quantum ecosystem in Amsterdam. This source of talent is what is currently lacking, and having access to that source is what we can contribute to the system.

[slide 25] These thoughts bring me to the third and last pillar of academic life for which I would like to sketch a vision, and that is *knowledge transfer* or *valorisatie* (in Dutch). *"Knowledge transfer (valorization) is regarded as the third core activity of Dutch universities, next to education and research. It is part of the day-to-day routine within the university: in start-ups and spin-offs where students, researcher and entrepreneurs mingle but also in a mix with education and research when student do internships or when researchers take on societal challenges or share their knowledge on TV or the internet."*[3] I believe that we will have a particular role to play in this respect in the area of quantum technologies.

[slide 26] Look at the amount of money that is globally invested into quantum technology at the moment. Clearly, there is a lot of HYPE in our area, and I see it as our task as scientists to keep the calm, and sketch a realistic picture of what can and cannot be done with quantum technology. In the end, these are exciting research questions that we would like to answer.

Also in the Netherlands, our research community has been quite successful in securing funding for this kind of research, both at the UvA, from NWO, from the EU, or from the national growth fund program. So, I'm confident that the next few years will be very quantum, and that it is the right strategy to invest in this technology now in order to remain among the front-runners in the future.

[slide 27] This holds for the major investments that the UvA and CWI have made into QuSoft, the local research center for quantum software, this also holds for the major investment of the national growth fund into this technology. Part of that money allows the UvA to construct a new *quantum building* with the main purpose of housing all people related to the quantum ecosystem in Amsterdam in one building. According to the current planning, it should be ready in 2026.

[3] from `https://www.universiteitenvannederland.nl/en_GB/knowledge-transfer.html`

In the quantum community, we often compare the developments in our field to the developments in AI. This is quite interesting, as the quantum field clearly lags behind AI by several years, we can learn a lot of lessons from what has happened in AI. The informatica institute of the UvA, my new home, has played a pioneering role in setting up the ICAI labs where industrial partners collaborate with AI researchers. For us quantum researchers, it is valuable to profit from IvI's previous experiences in this respect in AI. As chair of the network organization Quantum.Amsterdam, I will stay in close touch with these developments.

Looking Back

[slide 28] For me personally, it has been an amazing academic journey through at least three or four or five countries. I remember that about 20 years ago, when I was finishing my studies at ETH in Zurich, the scientific world looked very differently from today. I was a rare exception to write my diploma thesis in LaTeX, and I had to go to the library to look for scientific articles and books that they then had to order from some far-away place. I remember the repeated frustration when finally getting the material after a few days to find out that the ordered article was not relevant to my research question.

A lot has changed in these last 20 years, many researchers in our field write their own articles with LaTeXthat directly produces publishable output. Not without any fights, the importance of scientific publishers has diminished over this period, due to a push of open-access publishing and initiatives like Plan S. Sometimes, it takes a surprisingly long time until such "obvious ideas" are finally adopted. I have been lucky to work in a research field where we are following the high-energy physics attitude of making all our scientific papers freely available on the arXiv.

Also in terms of the scientific journey, I would not have dared to imagine as a mathematics student that I would end up standing here in front of all of you now. Back then, I was driven by scientific curiosity and the *pleasure and beauty of mathematics* and my interest in cryptography. I find it quite special that I could witness with my own eyes how this research field of quantum computing and cryptography has almost "exploded" over the last years, and that I now get the opportunity to further contribute and to shape this field in terms of research, education and knowledge transfer. These are extremely exciting times to be an active scientist in this area, as I will probably witness what this new technology can do for us in the future.

Acknowledgments

[slide 29] It is customary to end such an inaugural lecture with some words of thanks. I would like to start with thanking the executive board of the University of Amsterdam for my appointment as professor of Theoretical Computer Science (with special attention to quantum computing) as well as the dean, Peter van Tienderen, and my institute director, Alfons Hoekstra, for their efforts in the process of hiring me as professor here at this university.

In a wider context, I would like to thank all the people who have inspired me as math teachers, starting in high school in Switzerland, and then during my study of pure mathematics at ETH Zurich, and eventually my two PhD advisors Ivan Damgård and Louis Salvail (who is here today) during my PhD in Aarhus in Denmark. After my PhD, I came here to Amsterdam as postdoc in Harry's Algorithm & Complexity group. During these last 15 years, I have interacted scientifically with very many of you present here today. I would like to mention a couple of people by name:

1. Ulle Endriss: even though we have not interacted much scientifically, you have served me as role model in several respects. For example, in managing life as foreigner with a German-speaking background in this country, but maybe more in managing the politics of a research institute and an education program like the master of logic, and in how to professionally organize a faculty search procedure.
2. Serge Fehr: my fellow Swiss citizen. According to our publication records, we are each other's *favorite co-authors*, actually by far; which is not that surprising given that I basically followed you in terms of places throughout our careers, starting at ETH in Switzerland, going to Aarhus, and ending up here in Amsterdam, you at CWI, and I eventually at the UvA. Somehow it is fitting coincidence that you also held your own inaugural lecture in Leiden on Monday of this week. I'm pretty sure I'm not the only one who has you as role model of a *scientist par excellence*: you have a great sense for interesting problems, and with your razor-sharp mathematical precision and skills, you do not rest until you have fully understood the problem at hand, and until results are written up in the most accessible way. It is a pleasure to collaborate with you!
3. Ronald de Wolf: besides being the world expert in quantum algorithms and author of the ultimate lecture notes on this topic, and despite your appearances as *wolf in a yellow vest*, you are always well-informed about basically everything that happens in the world, and you remain a reliable moral compass in any academic matters, as well as my go-to reference for questions about the Dutch language.
4. Harry Buhrman is the reason why I came to Amsterdam in the first place, and he definitely played major roles on the long and winding road that led to me standing here. You are a visionary in the field of quantum, and you combined that with a good amount of *people skills* and *will power* to set up and lead QuSoft to what it is now. To me, you have been a great mentor in many respects.

I would like to thank friends and colleagues that made it here (or are watching online) from all over the world, especially those who travelled from far to be here to share this special moment with me.

I would like to thank my wife Sonja for the idea of producing some entertainment material for the kids present here today, and Feline Lindeboom for spending some hours on handcrafting all the cipher wheels this week. I hope they will have a positive impact on the youngest participants today.

Finally, I would like to thank my family, both the Swiss and Dutch parts of it: My brother who lives in Switzerland with whom I have spent a lot of time in my youth, and of course my mother and father who have allowed me to become the person that I am now. On the Dutch side, I would like to thank my wife's parents and her sister and their big families, who have so warmly embraced me into Dutch life here.

Finally, I would not be at this point without the support of my wonderful wife Sonja. You have been the stronghold on my side over all these years, from my simple life as postdoc in the Pijp in the core of Amsterdam, through all the years of job uncertainty, through the birth of our daughters Elin and Nova, our move to our own house on IJburg, and during our sabbatical semester in Berkeley two years ago. You have allowed me to focus and invest in important steps in my academic career, you are there to comfort me in stressful times, and you also help me to get my priorities in life clear. For all of this, I would like to say a big *"Thank You"* today. I am very happy to share today with you and our two wonderful daughters, Elin and Nova. The three of you are the most precious beings in my life. Thank you very much!

Ik heb gezegd.