May 30, 2016

Hyvät ystävät ja kollegat -- Dear friends and colleagues

Also on my behalf, I wish you welcome to this farewell event. I am glad to see here so many of the wonderful and devoted colleagues I have met and worked with during my years at TKK and Aalto. We have come here to celebrate the farewell of my professorship. But even more, it also puts a period on my whole working career. Let me start by giving an overview of it. How did I become a cryptologist?

After completing my PhD thesis and becoming a docent in Mathematics at the Faculty of Philosophy of University of Helsinki, I was already a mother of three children and I had to decide what to do when I grow up. When General Aimo Pajunen offered me the possibility to become a cryptology specialist with the Finnish Defence Forces I took the big leap from the realm of the university to a very different realm of a military organization. In the late eighties, cryptology was already an academically active research area. So I jumped on the moving train and it took me to a new world of research with new opportunities and challenges. I soon started publishing and some of my most cited papers date back to that time. For example, one of them identifies a function that was to become the S-box of the standard encryption algorithm AES.

Ten years later at TKK the research on network security had become very active and the importance of cryptology as one of its cornerstones became apparent. Initiated by Professor Arto Karila, a professorship in cryptology was established at TKK in 1997. About the same time, with the development of GSM the importance of cryptology was discovered at Nokia. They had recruited Doctor Valtteri Niemi, a student of Professor Arto Salomaa from Turku. A year later in 1998 Valtteri recruited me and I did not apply for the professorship at TKK.

At Nokia, I got an experience of modern industry, participated in standardization, and learned how to write and file patents. Nokia was a big player, and it opened us the opportunity to work together with renowned experts in a global scale. Together with N. Asokan we designed the new pairing protocol for Bluetooth and finalized it in collaboration with cryptographers from Microsoft. This protocol uses modern cryptography to hide the underlying complex mathematics from the user who simply needs to check the equality of two 6-digit numbers. Our protocol is running on all Bluetooth chips which in turn are placed in billions of devices to replace cables in short distance communication.

When the professorship in cryptology at TKK was open again in 2004, I did not hesitate to submit my application. I knew that this is what I want to do the rest of my working career. Without previous experience as a professor, I could not imagine how rich and rewarding time it was going to be. Without hesitation, the best thing has been the possibility to do research together with bright young minds. When catching up my research on cryptanalysis of symmetric key ciphers, the help and contributions of my PhD students and post docs were crucial. Thanks to Joo Cho and Miia Hermelin the contemporary tool box of symmetric key cryptanalysis now contains the method of multidimensional linear cryptanalysis. With Andrea Röck and Céline Blondeau we developed this new method further and discovered previously unknown links between linear and differential cryptanalysis. With Risto Hakala we studied applications to stream ciphers and actually succeeded to break one stream cipher proposal from industry. We also identified more exciting nonlinear functions for cryptography.

Cryptography is a wide area which provides not only symmetric key encryption algorithms but also other type of security mechanisms and protocols. My professorship has served as a contact point for cryptology in general and hosted researchers who work in other areas in cryptology just to mention Billy Brumley and

Kimmo Järvinen who are specialists in secure implementation of cryptographic algorithms.

Based on my experience, I strongly feel that this country needs a professorship in Cryptology also in the future. I hope that the recent efforts put forward by Camilla Hollanti and Pekka Orponen to get a new crypto professor in Aalto will be successful. The recent strengthening of the information security hub in Helsinki area improves the chances significantly.

There is still one important issue I want to address. It is how to attract female talent to computer science. I have had a few talented women researchers in my group. I do not think that it has happened just by accident but the fact that I am a woman has something to do with it. Last week, we had the pleasure to see a woman to become a laureate of the Millenium prize. In her speech, Professor Frances Arnold stressed that acting as a role model for female students has been one of the important aspects of her scientific career. She is right, the best way to encourage women to enter the technical fields is to give them role models.

Professor Arnold also expressed gratitude to her father, who had encouraged his daughter to study engineering by saying that if you become an engineer you will always have a job. My own father, himself an engineer, had a different opinion. He did not consider engineering suitable for women, but instead, encouraged me to become a math teacher. Now looking back, I feel that my life as a researcher and professor in computer science has actually been a great combination and offered both interesting work in engineering and technology as well as rewarding hours in classrooms with students. Referring to Professor Arnold's father, let me add that two of my daughters, Eeva and Katariina, have academic education in engineering – and so far they have always had a job.

The TKK which I entered eleven years ago was coming to its end, although not many people knew about it yet. Then organizational changes took place one after another until Aalto University eventually took its current shape. I am proud of having been a part of that development. As examples, I would like to mention the following functions and services that were introduced with Aalto and which I have found to work particularly efficiently in support of maintaining high standards in academic education and research:

- School of Science Doctoral Program Committee,
- HR coordination and recruitment support, and
- the tenure track system.

All good things come to an end. I started in 2005 knowing that I have at most eleven years to go. I wish to express my warmest thanks to you all for being there and helping me to make the best out of my short career as a professor.