The Isaac Newton Institute: A Personal Perspective

Peter Landrock, Founder of Cryptomathic

Peter Landrock grew up in Denmark and obtained his PhD in mathematics in 1974 from the University of Chicago. He began working on data security in 1984 whilst at Aarhus University, and built up one of the leading data security research teams within Europe. He founded Cryptomathic in 1986, one of the first companies to commercialise cryptographic algorithms, but it was his participation in the 1996 Isaac Newton Institute programme on Cryptology and Coding Theory that inspired him to leave academia and focus on the company. Always emphasising the importance of the underpinning mathematics, Cryptomathic went from strength to strength and is now one of the world's leading providers of security solutions to businesses across a wide range of industry sectors, including banking, government, technology, cloud and mobile.

In 2003, Cryptomathic was recognized by the World Economic Forum as a Technology Pioneer and, in 2004, it received the VISA Smart Star Award for its work on Chip and PIN.

In 2010, Peter Landrock was named by the European Patent Office as a Finalist for European Inventor in the "Lifetime Achievement" category. He has written several books and more than 70 articles on mathematics, cryptography, security and legal aspects of security. He has served as President of the International Association for Cryptological Research and remains on the Technical Advisory Board of the Microsoft Research Laboratory in Cambridge and the Scientific Board of NCCR Mobile Information Communication Systems, Switzerland.

"During the first 6 months of 1996 I was invited to be one of the organisers of the Isaac Newton Institute programme on *Computer Security, Cryptology and Coding Theory*. My co-organisers were Roger Needham, then Departmental Chairman of Cambridge University's Computer Laboratory and subsequently Director of Microsoft's Cambridge Research Laboratory, and Ross Anderson, now a Professor in Cambridge University's Computer Laboratory.

Attending the Newton Institute workshop, a new world opened in front of my eyes...

The following year I was still so inspired from my time at the Newton Institute that I decided to quit my position at Aarhus University and concentrate on my company

My background is in pure mathematics and physics and I studied for my PhD *On elementary abelian and dihedral defect groups* at the University of Chicago. But in 1984, after having spent a year at the Institute for Advanced Studies at Princeton, I started teaching cryptography to the students in Computer Science at Aarhus University in Denmark, where I held a position at the Mathematics Institute. I got very excited about this field and quickly made a career in cryptographic research and was elected President of the International Association for Cryptologic Research in 1992. It was on this background that I was invited to be one of the organisers for the 1996 cryptography programme at the Newton Institute.

Meanwhile, in 1986 I had started a small consulting company, Cryptomathic, in Denmark and just before I went to the Newton Institute we hired our first employees. The name was of course half a joke (Cryptomathic rather than Cryptomatic) and as a logo I chose a 4-dimensional hybercube projected onto the plane, an image that I had often used in the graduate courses I was teaching to illustrate representation theory of finite groups. Attending the Newton Institute workshop, a new world opened in front of my eyes, what with the researchers from universities and industry who participated, as well as the inspiration of the famous silicon fen environment, and I stayed the full six months of the programme. The following year I was still so inspired from my time at the Newton Institute that I decided to quit my position at Aarhus University and concentrate on my company. The company expanded and in 2000/01 we took in some investors, Maersk Data and Infineon Technologies. Maersk Data, the largest shipping company in the world, had taken an interest in our solution for Electronic Bills of Lading (legal documents between the shipper and carrier that list the type, quantity and destination of merchandise being carried), and Infineon were interested in our insight into cryptographic techniques and data security. I decided to build up a division of my company in Cambridge, first at St. John's Innovation Centre and later, as we grew in size, in the Cambridge Science Park and my wife and I moved permanently to Cambridge. Independent of this in 1997 I was asked to join the Technical Advisory Board of the new Microsoft Research Lab at Cambridge University.

I have maintained strong connections to the academic world and am a senior member of Wolfson College, but at the same time have managed to build a profitable company with about 60 employees. Of these about 50 have higher university education of at least 5–6 years, and about 25% have a PhD in computer science, mathematics, engineering or physics. Although most of them are employed in the original office in Denmark, where we do product development, innovation is handled by the Cambridge office under my supervision, where I work with some bright people I have hired from the University. We file almost all of our patent applications from the Cambridge office (approaching 15 by now), and the products we offer are in a nut shell: servers that are very secure and scalable for electronic banking; cryptographic functionality on debit- and credit chipcards as well as electronic passports; and advanced key management of cryptographic keys for very large banks and financial transaction players such as Barclays, VISA and Mastercard. The products are mainly based on our own cryptographic implementations, an exercise which can be mathematically challenging. Examples include elliptic curves in characteristic 2 or p, used e.g. by Cambridge Silicon Radio, a company specialising in connectivity, audio and location chips.

Since 2003, Cryptomathic has grown on average 20% year on year in turnover. In addition to our offices in Aarhus and Cambridge, we have an office in Munich, Germany near to Infineon Technology headquarters and have recently opened one in Silicon Valley, California: the USA is rapidly becoming our most important market.

We are proud of the fact that we have put advanced mathematics to work and of the extent that we are enabling our customers all over the world to build very secure and reliable solutions. They no longer rely on paper but use electronic information only, and if it had not been for my time at the Newton Institute, which was a real eye opener, I would probably never have had the courage to leave the secure world of research and teaching. Some of the ideas I got there helped Cryptomathic being nominated as one of the year's innovative companies in the world at the World Economic Forum in Davos in 2003. In 2010, I was furthermore nominated by the European Patent Office and the European Commission for the 2010 European Innovation Award for Lifelong Achievements in Cryptographic Techniques. I was slightly troubled by that nomination as it might be interpreted as a hint that it was about time to retire – which frankly is out of question. ”

Peter Landrock

We are proud of the fact that we have put advanced mathematics to work...and if it had not been for my time at the Newton Institute, which was a real eye opener, I would probably never have had the courage to leave the secure world of research and teaching.

Isaac Newton Institute for Mathematical Sciences
20 Clarkson Road, Cambridge, CB3 0EH, UK
tel: 01223 335999 **email:** info@newton.ac.uk **web:** www.newton.ac.uk

The Isaac Newton Institute is supported by EPSRC and other research councils, private foundations, companies and philanthropy.