Professor Jennifer Roma Seberry

Born in Camperdown, I grew up mainly in Rydalmere and Smithfield. I attended Parramatta High School and did a Science degree at UNSW with the help of a Commonwealth Scholarship.

In my career: I was the first person to teach cryptology at an Australian University (the University of Sydney), I am the first woman Professor of Computer Science in Australia. I was the first woman Reader in Combinatorial Mathematics in Australia (whilst at the University of Sydney).

I was a founding member of the University of Sydney's Research Foundation for Information Technology Information Security Group in about 1987. This grew, with many changes of name into the *Australian Information Security Association* an Australian representative industry body with over 1000 paid members and branches in most capitals. My much read paper "Mary Barrett, Karin Garrety and Jennifer Seberry, ICT professionals' perceptions of responsibility for breaches of computer security, *ANZAM'06, Aust and NZ Academy of Management*, Yeppoon, Qld, June 2006" (not covered by Google or Scopus but UOW downloads has details) was written using surveys of AISA meetings.

In my early career I concentrated on the the area known as Hadamard matrices which had special uses in the NASA space program to bring pictures back to Earth from space probes. Hadamard matrices are simply matrices which have entries which are $+1$ or -1 and are orthogonal. They are hard to find but have many important applications in securely transmitting information, providing bent functions for secure cryptographic codes, spectrography for chemical analysis and speeding engineering calculations which require transforms.

Their existence is still an unsolved question.

I was the first person to find an asymptotic bound for the existence of these structures: Jennifer Seberry Wallis, On Hadamard matrices, *J. Combinatorial Theory*, Ser. A., 18, (1975), 149-164. To do this I and other colleagues invented a whole new area of Discrete Mathematics, *Orthogonal Designs*, which later assumed great importance in mobile communications. My result was not improved for 20 years and then in 2005 a further improvement was found.

I have also been pioneering in the areas of Discrete Mathematics, such as "Bhaskar Rao Designs", "weighing matrices", and "directed symmetric balanced incomplete block designs". These areas are usually related to more efficient experimental designs. My other great interest is in "computer aided mathematics" again with a view to improving efficiency and reliability of computer related mathematics.

First at the University I started teaching cryptography and later formed a teams at ADFA@UNSW funded by Telecom for "Computer and Communications Security Research". A student member of the team was named Young Australian of the Year", and another received an award for his paper on "Smart cards" (the forerunner of all those chip credit cards). When I joined the University of Wollongong I put

together a team, known as *Centre for Computer Security Research* to provide a reservoir of expertise for computer security. While I directed the Centre for Computer and Communications Security Research it built a secure WAN for the University of NSW campus using the LOKI encryption algorithms and secure protocols developed within my group. Although this has now been decommissioned it never was hacked or broken into. Fifteen of my PhD students have contributed to university education in cryptography, mathematics, statistics and electrical engineering. I have also been active supervising Masters and honours students. I concern myself with mentoring and guiding both junior staff and students. I provide opportunities for them to gain experience by having developed a series of conferences "The 26th Australasian Conference on Combinatorial Mathematics and Combinatorial Computing" and the "Sixteenth Conference on Information Security and Privacy", both held this year, are continuations of conference series I have founded or co-founded. I have edited, refereed and contributed to numerous international and national journals, conferences and distinguished lectures.

In the early 2000s I was involved in research dealing with optimization of orthogonal spreading sequences for CDMA systems. That work resulted in many journal and conference publications and the developed families of orthogonal sequences are often cited as the sequences having the best correlation properties among known sets. My work was later extended to application of orthogonal designs in construction of complex orthogonal space-time codes that can be used in modern MIMO wireless communication systems to improve performance in case of fading channels and to improve systems' capacity. This has led to a new field of orthogonal amicable designs over complex and quaternion fields.

I have written over 450 research publications, successfully supervised 30 PhD students, 7 Masters Research Honours theses and 20 Honours undergraduate theses.

I am a Fellow of the Australian Computer Society, a Fellow of the Institute of Mathematics and its Applications (Britain), A Fellow of the Institute of Combinatorics and its Applications (Canada), a Chartered Mathematician (British Council) and I was recently made a Fellow of the International Association for Cryptologic Research for "outstanding contributions to research and education in cryptologic research and education and for fostering the Australian research community".

My father and grandfather were psychiatric nurses.

I love choir music and have belonged to a number of church and cathedral choirs. Because of my background I have always felt and empathy for the working poor and the mildly mentally ill. I am very involved in a program to encourage high school students to keep up their mathematics as so many career paths close without maths.

Jennifer Seberry
Professor of Computer Science
University of Wollongong
12 September 2012.