

## Curriculum Vitae

### Dr Braden Phillips

Ph.D., B.E.(Hons), B.Sc., MIEEE

School of Electrical & Electronic Engineering  
The University of Adelaide  
ADELAIDE, SA, 5005  
AUSTRALIA

Work: +61 (08) 8303 5114

Fax.: +61 (08) 8303 4360

E-Mail: Braden.Phillips@adelaide.edu.au

Date of Birth: 6 September 1971

Nationality: Australian

### Employment History

5/2003–

*Senior Lecturer*

School of Electrical & Electronic Engineering  
The University of Adelaide

9/2000–9/2002

*Lecturer*

Division of Electronic Engineering  
Cardiff University

7/1998–6/2000

*Part Time Lecturer*

Department of Information Technology Studies  
Adelaide Institute of TAFE

12/1995–6/2000

*Manager/Engineer*

Current Dynamics, Unley

11/1991–12/1994

*Project Engineer*

Automation and Process Control Services, Stepney

### Education

1994–2000

*Ph.D.*

The University of Adelaide

1989–1993

*B.Eng. (Hons) (Electrical & Electronic Engineering)*

The University of Adelaide

1989–1992

*B.Sc. (Mathematics & Computer Science)*

The University of Adelaide

2000

*Certificate IV, Assessment & Workplace Training*

Adelaide Institute of TAFE

## **Continuing Education**

3/2008	<i>ECMS Development program: building our future capability</i> 3-day course, Kerrie Ashcroft & Stewart Mitchell
8/2005	<i>Mentoring the mind</i> 10-hour course, Anama Morriss & Rosanne DeBats
2/2004–5/2004	<i>Advanced French</i> Weekly lessons, Alliance Française, Adelaide
8/2003–9/2003	<i>Teaching at University</i> Learning and Teaching Development Unit, The University of Adelaide
9/2002	<i>Intermediate French</i> 1-week course, Accent Français, Montpellier, France
9/2001–9/2002	<i>Intermediate French</i> Weekly lessons, Cardiff City Council, UK
2/2000–6/2000	<i>Beginning French</i> Twice-weekly lessons, Alliance Française, Adelaide

## **Research**

### **Research Interests**

Digital Arithmetic	Hardware for integer and floating point operations, number systems, estimating arithmetic
Information Security	Implementing cryptography, circumventing side-channel attacks, semiconductor remanence
Digital Microelectronics	Low-power and high-performance circuits
Computer Architecture	Data value speculation, application specific architectures

### **Principle Research Projects**

Arithmetic data value speculation  
RNS hardware for public-key cryptography  
Semiconductor remanence

### **Invited Presentations**

*Conference Workshop*, The Mathematical Association of South Australia, Annual Conference, “Faster, smaller, more efficient: how computers do arithmetic”, Adelaide, Australia, 24 April 2009.

*Conference Workshop*, The Mathematical Association of South Australia, Annual Conference, “Formulating Electronics Problems for Mathematical Studies”, Adelaide, Australia, 23 April 2008.

*Invited Visit*, LIRMM, The University of Montpellier II, “Estimating arithmetic”, Montpellier, France, December 2007.

*Conference Presentation*, Advanced Signal Processing Algorithms, Architectures, and Implementations XVI, “Estimating adders for a low density parity check decoder”, San Diego, CA, USA, 15 August 2006.

*Conference Presentation*, 35th Asilomar Conference on Signals, Systems and Computers, “Modular multiplication in the Montgomery residue number system,” Pacific Grove, CA, USA, 7 November 2001.

*Conference Presentation*, 34th Asilomar Conference on Signals, Systems and Computers, “Optimized squaring with sliding windows,” Pacific Grove, CA, USA: IEEE, Piscataway, NJ, USA, October 30 2000.

*Seminar*, Agere Systems, “Optimised Squaring of Long Integers using Precomputed Partial Products,” Bell Laboratories, Holmdel, NJ, USA, June 2001.

### **Consulting & Contract Research**

4/2007	<i>Semiconductor remanence (experimental investigation)</i> The Defence Science and Technology Organisation
1/2006	<i>Semiconductor remanence (literature survey)</i> The Defence Science and Technology Organisation
10/2005	<i>Expert opinion on a legal matter</i> Thomson Playford
1/2005	<i>Embedded software for a Bluetooth device</i> Don Alan Electronics

### **Grants and Funding**

2007–2010	<i>Smart sensors for smart packaging</i> \$307000, Premier’s Science and Research Fund
2005–2007	<i>RNS Hardware for public-key cryptography and e-security</i> \$160000, ARC Discovery Grant

2007	<i>Xtensa software</i> Tensilica University Program
2006	<i>Student project: hardware implementation of a Reed Solomon decoder</i> \$2000, Agere Systems
2006	<i>Student microchip fabrication</i> \$8000, MOSIS Educational Program
2005	<i>Student project: clock tree insertion</i> \$2000, RADLogic
2005	<i>Arithmetic data value speculation</i> \$2000, ECMS Overseas Conference Leave Scheme
2005	<i>Student microchip fabrication</i> \$8000, MOSIS Educational Program
2005	<i>Arithmetic unit design for data value speculation</i> \$5500, ECMS Small Research Grants Scheme
2004	<i>Tornado software</i> Wind River University Teaching Grant
2004	<i>Student microchip fabrication</i> \$8000, MOSIS Educational Program
2003	<i>Scaling and reduction in the residue number system with pairs of conjugate moduli</i> \$1200, ECMS Overseas Conference Leave Scheme
2002	<i>Equipment for a microprocessor teaching laboratory</i> \$US6000, Texas Instruments Donation
2001	<i>Smart-card architectures for public key cryptography</i> £6500, ENGIN Seedcorn Research Fund, Cardiff University
2001	<i>Optimised squaring of long integers using precomputed partial products</i> \$1700, Royal Society Travel Grant

## **Postgraduate Research Students**

### **Past Research Students**

Yinan Kong	<i>RNS hardware for public-key cryptography and e-security</i> Ph.D., completed 2009
Tristan Newby	<i>Evaluation of the Cell processor for implementation of the Annex system</i>

	M.Sc. (Defence), completed 2008 (DSTO supervisor: C. Owen)
Damith Ranasinghe	<i>Security issues in RFID systems</i> Ph.D., completed 2007 (first supervisor: P. Cole)
Hooman Nikmehr	<i>Algorithms for floating point division</i> Ph.D., completed 2005 (first supervisor: C. C. Lim)
Yann Bergot	<i>Wavelet transform vs. edge detector algorithms applied to the detection of iris boundaries in photographs of eyes</i> M.Sc., Cardiff University, completed 2000
Stephane Ramon	<i>Design of a 1024-bit self-timed adder based on RSFQ technology for RSA decryption systems</i> M.Sc., Cardiff University, completed 2000
Salma Alderazi	<i>A study of the optimal Rademacher Walsh transform technique for single stuck-at faults in digital circuits</i> M.Sc., Cardiff University, completed 2000 (first supervisor: P. Rayment)

#### **Current Research Students**

Robert Moric	<i>Fault tolerance</i> Ph.D., commenced 2008
James Kitchener	<i>Online arithmetic in cryptographic functions</i> Ph.D., commenced 2007
Zhining Lim	<i>An RNS-enabled microprocessor</i> Ph.D., commenced 2006
Daniel Kelly	<i>Arithmetic data value speculation</i> Ph.D., commenced 2005
Norfadila Mahrom	<i>Chip Multi-Processor: Optimizing Memory Sharing Mechanisms</i> Ph.D., commenced 7/2008 (first supervisor: M. Liebelt)
Geng Tian	<i>Low Power Computer Architecture</i> Ph.D., commenced 7/2009 (first supervisor: M. Liebelt)
Raja Ghosal	<i>Lightweight cryptography</i> M.Eng.Sc., commenced 2006 (first supervisor: P. Cole)

#### **Theses Examined**

Jeng Howe Kong	<i>Design and analysis of a visual programming language for PIC microcontrollers</i> M.Eng.Sc., The University of Adelaide, 2/2004
----------------	---

Yodachai Wongsuwan     *Low power performance of primitive operator digital filters*  
Ph.D., Cardiff University, 6/2003

### **Teaching**

3/2007–     *1009 Electrical & Electronic Engineering 1A*  
Lecturer, Course Coordinator 2009, The University of Adelaide (18 contact hours, 400 students)

3/2004–     *7051 Microelectronic Datapaths and Arithmetic*  
Course Coordinator, The University of Adelaide (34 contact hours, 15 students)

3/2004–     *4037 Digital Microelectronics*  
Course Coordinator, The University of Adelaide (28 contact hours, 100 students)

7/2003–11/2006     *3022 Real Time Systems IV*  
Course Coordinator, The University of Adelaide (30 contact hours, 50 students)

9/2000–9/2002     *EN2063 Analogue and Digital Electronics*  
Module Leader, Cardiff University (34 contact hours, 80 students)

9/2001–9/2002     *EN1068 Laboratory 1 and EN1070 Laboratory 2*  
Module Leader, Cardiff University (96 contact hours, 80 students)

1/2001–6/2002     *EN3802 VLSI Systems*  
Lecturer, Cardiff University (18 lectures, 35 students)

9/2000–9/2001     *EN1068 Laboratory 1 and EN1070 Laboratory 2*  
Laboratory Demonstrator, Cardiff University (48 contact hours, 80 students),

1/2001–6/2001     *EN3056 Industrial Computer Control Systems*  
Lecturer), Cardiff University (8 lectures, 50 students)

7/1998–6/2000     *N1: Using a Personal Computer*  
*Computer Systems Basics*  
*Installing and Managing a GUI*  
*Introduction to Local Area Networks*  
Instructor, Adelaide Institute of TAFE (128 contact hours p/a, 20 students)

7/1998–6/2000     *N3: Wide Area Networks*  
*Developing Batch Files*  
*PC Peripheral Devices*

	<i>PC Support</i> Instructor, Adelaide Institute of TAFE (128 contact hours p/a, 20 students)
1996	<i>Unix for Users</i> Industry Trainer, Communicata Systems (3-day course)
1994–1996	<i>Mathematics and Electronics</i> Tutor, The University of Adelaide
1994–1995	<i>PLC Programming</i> Industry Trainer, APC Services (2 5-day courses)

## **Professional and Community Service**

<b>Affiliations</b>	Member of the IEEE  Centre for High Performance Integrated Technologies and Systems, (CHiPTec), The University of Adelaide
---------------------	--

## **Professional Activities**

10/2008	Technical Session Chair, Forty Second Annual Asilomar Conference on Signals, Systems, and Computers
2004–	Conference Technical Committee, SPIE International Symposium on Smart Materials, Nano-, and Micro-Smart Systems
12/2008	Technical Session Chair, Smart Structures, Devices, and Systems IV
12/2006	Technical Session Chair, Smart Structures, Devices, and Systems III
10/2006	Technical Session Chair, Fortieth Annual Asilomar Conference on Signals, Systems, and Computers
12/2004	Technical Session Chair, Smart Structures, Devices, and Systems II  <i>Journal peer reviewer:</i> IEEE Transactions on Computers; IEEE Transactions on Circuits and Systems (I & II); IEEE Transactions on VLSI Systems; IEE Proceedings; IET Circuits, Devices & Systems; Security and Communication Networks

## **University Service**

1/2009–	Associate Dean (Information Technology), Faculty of ECMS
---------	--

1/2008– Program Leader, Bachelor of Engineering (Computer Systems)

**Other**

3/1999–6/2000 Parish Council, St. Andrew’s Church, Walkerville

**Awards**

1993 IRE Student Prize for Public Speaking

1988 Matriculation Merit Certificates: Physics & Chemistry

1987 Wainwright Prize for Chemistry

**Publications**

Please refer to the list of publications attached.

The University of Adelaide, September 2009