

**ICE-EM RSA 2007 Cryptography Workshop**  
on  
***Pairing Based Cryptography***  
held at QUT, Brisbane, 27-29 June 2006

**SUMMARY**

This was the second joint workshop between RSA and the International Centre of Excellence for Education in Mathematics (ICE-EM). The aim for this workshop was to hold discussions lead by experts on the latest issues pairing based cryptography.

**Overview of Workshop**

The purpose of this workshop was to inform attendees of latest developments and research challenges in the area of pairing based cryptography. National and international researchers and postgraduate students as well as industry practitioners were encouraged to attend.

The past five years have witnessed an explosion of interest in public key cryptography based on elliptic curve pairings. The bilinearity property of such pairings has enabled a range of new cryptographic primitives which could not be realised previously, most prominently identity-based cryptography. This workshop will bring together international and national experts to discuss pairings and their applications to cryptography. Topics included:

- Mathematical foundations
- Implementation issues
- Cryptographic protocols

**Keynote lecturers were presented by:**

- Prof Kenny Paterson, Royal Holloway, London
- Dr Xavier Boyen, Voltage Security Inc, USA
- Dr Andreas Enge, Ecole Polytechnique, France
- Dr Michael Scott, Dublin City University, Ireland
- Prof Willy Susilo, University of Wollongong, Australia

The workshop was well attended. A total of 46 delegates attended the workshop.

This consisted of:

- 23 research students from Australia,
- 9 academic staff
- 4 overseas delegates
- 5 RSA Sponsor attendees



## ICE-EM RNSA 2007

[Workshop Information  
and Reception](#)  
[Contact Us](#)  
[Invited Speakers](#)  
[Registration](#)  
[Hotel Information](#)  
[Lecture Program](#)  
[Intensive Short Course](#)  
[Venue Information](#)

### Related Conferences

[ACISP 2007](#)

[Pairing 2007](#)

## Intensive Short Course - Draft Program

- The course will be held over two days (June 25, 26).
- Format for each day is four 1.5 hour sessions.
- Each 1.5 hour session may consist of 1 hour lecture plus 0.5 hour tutorial (split depends on topic and presenter).

### Monday 25 June

0845-0900: *Registration*

0900-1030: **Introduction to Public Key Cryptography I** (Colin Boyd)

1030-1100: *Coffee*

1100-1230: **Introduction to Public Key Cryptography II** (Colin Boyd)

1230-1330: *Lunch break*

1330-1500: **Introduction to Elliptic Curves I** (Huseyin Hisil)

1500-1530: *Tea*

1530-1700: **Introduction to Elliptic Curves II** (Huseyin Hisil)

### Tuesday 26 June

0845-0900: *Registration*

0900-1030: **Implementation of Elliptic Curve Cryptography** (Huseyin Hisil)

1030-1100: *Coffee*

1100-1230: **Basics of Pairings** (Colin Boyd)

1230-1330: *Lunch break*

1330-1500: **Basics of ID-based Cryptography** (Juan Gonzalez Nieto)

1500-1530: *Tea*

1530-1700: **Basics of ID-based Cryptography** (Juan Gonzalez Nieto)

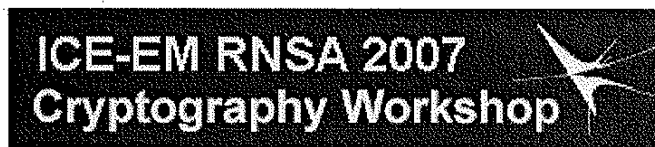
### Sponsors:



INTERNATIONAL CENTRE  
OF EXCELLENCE FOR  
EDUCATION IN  
MATHEMATICS



Research Network  
a Secure Australia  
Protecting Australia



## ICE-EM RNSA 2007

[Workshop Information  
and Reception](#)  
[Contact Us](#)  
[Invited Speakers](#)  
[Registration](#)  
[Hotel Information](#)  
[Lecture Program](#)  
[Intensive Short Course](#)  
[Venue Information](#)

### Related Conferences

[ACISP 2007](#)

[Pairing 2007](#)

## International Lecture Series - Draft Program

### Wednesday 27 June

0945-1000: *Welcome*  
 1000-1100: **Mike Scott: Introduction to pairings** [Slides]  
 1100-1130: *Coffee*  
 1130-1230: **Xavier Boyen: Introduction to identity-based encryption** [Slides]  
 1230-1400: *Lunch break*  
 1400-1500: **Kenny Paterson: Pairing-based cryptography in the standard model** [Slides]  
 1500-1515: *Short break*  
 1515-1615: **Xavier Boyen: Pairing-based signatures** [Slides]  
 1615-1630: *Short break*  
 1630-1730: **Willy Susilo: Fuzzy identity-based encryption**  
 1800-2000: *Reception sponsored by RSA*

### Thursday 28 June

0930-1030: **Mike Scott: Implementation of pairings** [Slides]  
 1030-1100: *Coffee*  
 1100-1200: **Kenny Paterson: Certificateless cryptography I** [Slides]  
 1200-1330 *Lunch*  
 1330-1430: **Xavier Boyen: Complexity assumptions from pairings** [Slides]  
 1430-1445: *Short break*  
 1445-1545: **Mike Scott: Looking for pairing-friendly curves** [Slides]  
 1545-1615: *Tea*  
 1615-1715: **Juan Gonzalez: ID-based key agreement**

### Friday 29 June

0930-1030: **Andreas Enge: Subexponential discrete logarithm algorithms**  
 1030-1100: *Coffee*  
 1100-1200: **Kenny Paterson: Certificateless cryptography II** [Slides]  
 1200-1330: *Lunch*  
 1330-1430: **Andreas Enge: Constructing pairing-friendly**