## 1. BYLAW CHANGE

SHALL the Bylaws of the International Association for Cryptologic Research, Inc. be changed to (1) add that only the Officers and Elected Directors vote for the appointment of Program Chairpersons, and (2) to update headings and layout for clarity?

A full copy of the Bylaws reflecting the proposed changes can be found online at http://www.iacr.org/elections/2005/ProposedBylaws.html.

➥ **Vote** by marking like this ☑ beside your response.

□ YES (change the Bylaws)

□ NO (do not change the Bylaws)

## 2. THREE DIRECTORS

Election is being held for three (3) directors for the IACR Board of Directors. These directors will serve a three-year term from 1 January 2006.

Names are presented in a shuffled order. Candidates' statements (in the same order) may be found on the reverse of this page.

➥ **Vote** by marking like this ☑ beside your selections.

### Director (vote for no more than three):

□ Kwangjo Kim

□ Antoine Joux

□ Greg Rose

□ Yvo Desmedt

□ Stuart Haber

## 3. RETURN YOUR BALLOT

➥ **Seal your completed ballot in the small envelope** marked "Ballot". Do not write anything on the small envelope. This will preserve anonymity of your vote.

➥ **Seal the small envelope in the large envelope** with the printed address of the Returning Officer (Arjen K. Lenstra).

➥ **Print your name and place your signature on the large envelope.** This is very important. It is used to authenticate your vote.

➥ **Send the large envelope to the returning officer.** Only ballots received by midnight (EST) on 15 November 2005 will be counted. You may need to use Air Mail. Be sure to attach sufficient postage.

## CANDIDATES' STATEMENTS

**Kwangjo Kim:** For the past 20 years, I have successfully served on various committees of IACR conferences and workshops, including General Chair of Asiacrypt2004 and Asiacrypt Steering Committee Chair. If elected, I will be committed to narrowing the gap in our academic achievements and promoting understanding of cultural differences. Vote for me.

Home page: http://vega.icu.ac.kr/~kkj

Longer statement: http://vega.icu.ac.kr/~kkj

**Antoine Joux:** I have been a regular member of IACR since 1990 and have regularly contributed to IACR conferences. I would like to participate in the strategic direction of our community. I intend to make sure that researchers can easily attend conferences thus keeping IACR focused toward scientific excellence and worldwide recognition.

Longer statement: http://www.prism.uvsq.fr/~joux/IACR_statement.htm

**Greg Rose:** I believe in giving back to organizations that have helped me, and IACR has done so. Organizations I have helped in the past include USENIX, the Inner City Montessori Association, the Australian Unix Users Group, the System Administrators Guild and General Chair of Crypto 2003.

Home page: http://people.qualcomm.com/ggr

Longer statement: http://people.qualcomm.com/ggr/iacr.html

**Yvo Desmedt:** IACR promoted research internally (workshops, fellows, best paper awards). Local issues in certain countries (as the lack of grants on hash function in the US) require local chapters. IACR should maintain the high visibility of its publications. Wherever you may live, I am listening to your input. Vote for me.

Home page: http://www.cs.ucl.ac.uk/staff/Y.Desmedt/

Longer statement: http://www.cs.ucl.ac.uk/staff/Y.Desmedt/IACR/

**Stuart Haber:** I have served on the Board for the past two years as General Chair of Crypto 2005, and would like the opportunity to help keep the IACR going on an even keel, advance the scientific interests of its members, and help us to deal intelligently with questions surrounding electronic publication.

Home page: http://www.hpl.hp.com/personal/Stuart_Haber/

Longer statement: http://www.hpl.hp.com/personal/Stuart_Haber/iacr-bod-statement.html