



IACR Fellows Ceremony
Crypto 2012

www.iacr.org



***IACR Fellows Program (•2002):
recognize outstanding IACR members for
technical and professional contributions that:***

- Advance the science, technology, and practice of cryptology and related fields;
- Promote the free exchange of ideas and information about cryptology and related fields;
- Develop and maintain the professional skill and integrity of individuals in the cryptologic community;
- Advance the standing of the cryptologic community in the wider scientific and technical world and promote fruitful relationships between the IACR and other scientific and technical organizations.



IACR Fellows Selection Committee (2012)

- Arjen Lenstra (EPFL)
- Ueli Maurer (ETHZ), chair
- Kevin McCurley (Google Inc)
- Tatsuaki Okamoto (NTT research)
- Ron Rivest (MIT)



Current IACR Fellows

- Tom Berson
- G. Robert Jr. Blakley
- Gilles Brassard
- David Chaum
- Andrew Clark
- Don Coppersmith
- Ivan Damgård
- Yvo Desmedt
- Whitfield Diffie
- Oded Goldreich
- Shafi Goldwasser
- Martin Hellman
- Hideki Imai
- David Kahn
- Arjen K. Lenstra
- James L. Massey
- Ueli Maurer
- Kevin McCurley
- Ralph Merkle
- Silvio Micali
- Moni Naor
- Jean-Jacques Quisquater
- Michael O. Rabin
- Charles Rackoff
- Ron Rivest
- Richard Schroepel
- Adi Shamir
- Gustavus (Gus) Simmons
- Jacques Stern
- Scott Vanstone
- Andrew Yao



New IACR Fellows in 2012

- Mihir Bellare
- Eli Biham
- Manuel Blum
- Andrew Odlyzko
- Phil Rogaway
- Claus Schnorr
- Jennifer Seberry



Mihir Bellare

IACR Fellow, 2012

- For fundamental contributions to the theory and practice of cryptography and for educational leadership in cryptography





Andrew Odlyzko

IACR Fellow, 2012

- ✚ For pioneering contributions to cryptography and for service to the IACR





Claus Schnorr

IACR Fellow, 2012

- For fundamental contributions to the design and analysis of cryptographic systems





Eli Biham

IACR Fellow, 2012

- For fundamental contributions to cryptanalysis, including the co-invention of differential cryptanalysis

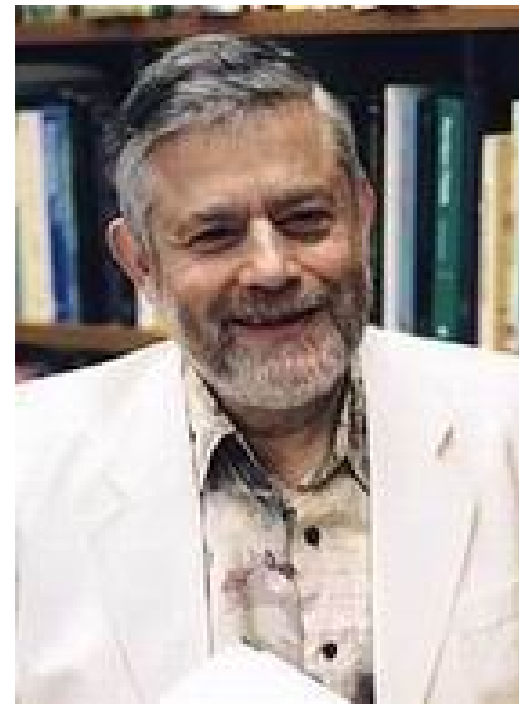




Manuel Blum

IACR Fellow, 2012

- For pioneering modern cryptography and for sustained contributions to cryptographic education





Phil Rogaway

IACR Fellow, 2012

- For fundamental contributions to the theory and practice of cryptography and for educational leadership in cryptography





Jennifer Seberry

IACR Fellow, 2012

- For outstanding contributions to cryptologic research and education, and for fostering the Australian research community





Nominations for 2013 are encouraged

- Candidates, nominators, and endorsers must be IACR members. Verify membership by corresponding with [iacrmem\(AT\)iacr.org](mailto:iacrmem(AT)iacr.org)
- Submit to [fellows\(AT\)iacr.org](mailto:fellows(AT)iacr.org)
- Deadline: December 31, 2012
- Detailed instructions at <http://www.iacr.org/fellows/>



IACR Fellows Selection Committee (2013)

- Arjen Lenstra (EPFL), chair
- Ueli Maurer (ETHZ)
- Kevin McCurley (Google Inc)
- Ron Rivest (MIT)
- Phil Rogaway (UC Davis)