



UMass Lowell Computer Science Colloquium Announcement

Speaker: Dr. David Chaum
Founder and a member of the Board of Directors of DigiCash Inc.,

Date & Time: June 6, 2003 (Friday), 3:00pm-4:00pm

Place: Olsen 311. Refreshments are served at 2:45pm

Secret-Ballot Receipts and Transparent Integrity

Receipts showing exactly whom you voted for -- just what is generally wanted and expected today - - have been outlawed to prevent vote selling and other abuses. A new kind of receipt cannot be abused. It also lets you be sure that your votes are correctly included in the final tally, even if all the computers used to run the election are compromised!

Receipts are printed on two-layer media by a modified version of familiar receipt printers. You can read them clearly in the booth; but before leaving, you must separate the layers and choose which one to keep. Either one you take has coded in it the vote information you saw, though your choices can now only be read using keys divided among computers run by election officials.

The layer you take is supplied by the voting machine for publication on an official election website, where you can verify that it is posted. After deriving the tally from the posted receipts, a lotto-like draw selects parts that must be decrypted for inspection, but not so many parts that privacy is compromised. Anyone with a computer can simply check all the decryptions, which should also be published on the website, and thereby verify that the final tally must be correct.

The printers and media are practical and under development. The overall system cost is lower than with today's voting machines and the hardware can additionally be used for other purposes year round. Current election system functionality, including write-ins and provisional ballots, is fully supported and can be extended significantly. A variety of public policy issues are raised. (See www.vreceipt.com.)

Brief Bio: Dr. David Chaum holds many patents in cryptographic protocols including several inventions on blind signatures. The following information is from <http://www.chaum.com/>:

Dr. David Chaum is the founder and a member of the Board of Directors of DigiCash Inc., a company that has pioneered electronic cash innovations.

He received his Ph.D. in Computer Science, with a minor in Business Administration, from the University of California at Berkeley and taught at New York University Graduate School of Business Administration and at the University of California. He built up a cryptography research group at the Center for Mathematics and Computer Science (CWI) in Amsterdam and during this time also founded DigiCash. In 1993, he left CWI to become CEO of DigiCash, which had doubled in size since its founding in 1990 with 12 employees.

In the area of cryptography, he has published over 45 original technical articles (see list of articles), received over 17 US patents, and founded the scientific organization, the International Association for Cryptographic Research (IACR). Concurrently he created and chaired the Smart Card 2000 conferences and several European Union funded industry consortia, including CAFE, which focused on electronic-wallets and the smart cards they hold..

Professional recognition includes invited articles featured in *Scientific American* (August '92) and *Communications of the ACM* (February '81), EU Technology Innovations Award ITEA '95, D.A.A.D. and UC Regents Fellowships. He has appeared often in popular and trade media, and is widely consulted on matters of cryptography, payments policy and overall technology direction.

Colloquium Coordinator: *Jie Wang*, wang@cs.uml.edu. Website: <http://www.cs.uml.edu/~wang/colloquia/>