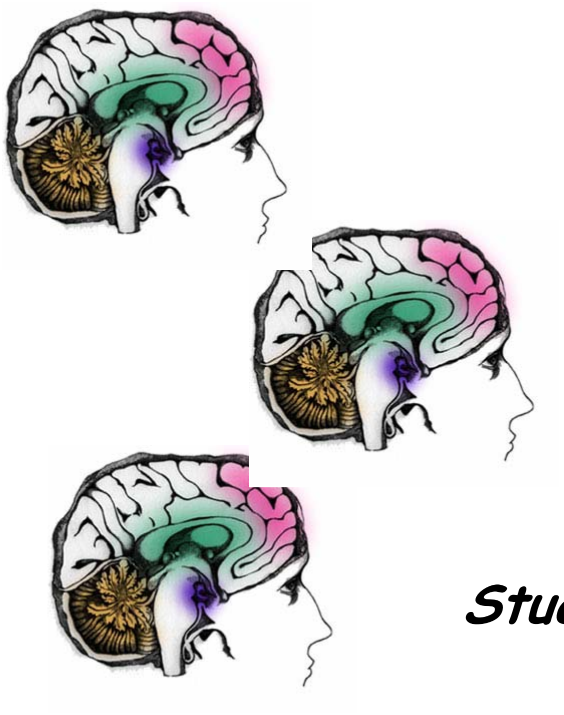
# Secure Distributed *Human* Computation



**Zulfikar Ramzan**

DoCoMo Labs USA

*Collaborators:*

*Craig Gentry (DoCoMo Labs USA)*
*Stuart Stubblebine (Stubblebine Labs)*

Rump Session, Asiacrypt 2004

# Large-Scale Distributed Computation

The Internet enabled the possibility of creating a giant distributed computing system by harnessing idle CPU cycles around the world.

Notable examples include:

- ✓ SETI@Home's search for extra terrestrials.
- ✓ Entropia.com's Giant Internet Mersenne Prime search.
- ✓ Distributed.net's cryptosystem attacks.

Of course, many problems are difficult for even very powerful computers; e.g., "AI-complete problems" from:

- ✓ Natural language processing;
- ✓ Image analysis;
- ✓ Voice analysis, etc, etc.

Perhaps instead of only having computers be end clients in a distributed system, we should also consider having *human* clients….

Maybe this sounds crazy… but…

# Examples of Dist. Human Computation…

- Vipul's razor
  - ✓ Collaborative filtering product for anti spam
  - ✓ If enough humans vote that email is spam, it's thrown in junk folder
- Finding solutions to CAPTCHAs.
  - ✓ CAPTCHAs: puzzles seen when registering for free email accounts.
  - ✓ Spammers who want to create spamming accounts get humans to solve these captchas in exchange for illicit content.
- ESP game
  - ✓ Two humans in different locations are shown same image.
  - ✓ Each is asked to submit words that describe image. If words are both same, then points are received.
  - ✓ At the end, game owner has labels for many pictures (useful for image search)
- Cyphermint check cashing kiosks (located in public places).
  - ✓ Humans at "back end" perform facial recognition to prevent fraud.

# Relations to Crypto/Security + Other Fields

*"Cryptography is concerned with the construction of schemes that withstand any abuse. Such schemes are constructed so as to maintain a desired functionality, even under malicious attempts aimed at making them deviate from their prescribed functionality."*

*-Oded Goldreich*

Not quite Secure Multi-party computation:

- ✓ Human vs. computer clients; provide candidate answers vs. function inputs.
- ✓ Computation may be facilitated by semi-trusted server'
- ✓ Input privacy may be less relevant.
- ✓ Answer may not be clear cut.

Also related to:

- ✓ E-cash
- ✓ Distributed Computation with Payout
- ✓ Voting
- ✓ Reputation Systems

In general, some interesting questions security/crypto as well as in Algorithms (how to redesign algos for human input) and Human Computer Interaction (how to design interfaces).

# Preliminary Thoughts and Final Remarks

- Can show majority vote of humans is better (more secure) than Bayesian Combination of Classifiers.
- Can use basic decision theory tools to derive design principles for Distributed Human Computation schemes for deterring cheaters.
  - ✓ Give human clients a rating and provide payouts for correct answers that are proportional to this rating.
  - ✓ Decrease client rating substantially for errors, but increase it slowly for correct answers
  - ✓ Monitor “high-utility” for cheating situations more carefully.

*Overall, this seems to be an untapped research area, and could hold much promise for interesting research questions and directions.*