PROVE HONESTY OF ORGANIZATION

Install confidence in participants

Current practice

- Hands are generated using BigDeal program
- BigDeal is so far seen as safe and fair

- However, nobody can check that the organization is honest
- They(Maurizio) could just enter the hands manually

Potential problem

- Participants could be suspicious about the hands, and there is no way that the organization can prove they did not cheat

- Does this problem ever exist? If not we can stop now.

How BigDeal works

- Generate big random number(160 bits)
- Generate hands from this number

- If we use BigDeal once per session, and do not look it is OK
- But we could redeal if we don’t like the hands, or rearrange sessions so the wildest hands are in the evening session, or …

Possible modification to dealing process

- Make big random number differently
- Generate hands as usual
- Make it possible **afterwards** to check the hands

Short mathematical interlude

- The proposal we are about to make uses the concept of a cryptohash, or hash for short
- A hash is a function that turns an arbitrary amount of information into a fixed length string
- So for example hash(“Giannarigo”) = d4de8bf350b0e4910efe2e28d54ed5af0d71e4f09b3024088bb23abecac92448
- This is easy to compute, but it is “impossible” to take the hash and come up with “Giannarigo”
- The official term for “impossible” is “computationally infeasible”

What must we achieve?

- The Tournament organiser should lose his option to select hands, or sets of hands. He must be restricted.
- The public should be able to check on this afterwards.
- Of course the hands should still conform to the normal variability.

- The last is easy. Whatever unique starting value you give to BigDeal it will conform.

First attempt at new process

- The TO generates the keys for all sessions in advance of the tournament.
- Of course he does not publish the keys, but he ***does*** publish the hash of the keys.
- The public cannot generate the hands before the tournament, since they cannot make the keys from the hash.

- After the tournament the TO publishes the keys, and the public can check that the hash is correct.
- This proves the TO did not fiddle with the hands ***after*** publication.

Second attempt (1)

- The first attempt is of course not good enough, since the TO can fiddle the hands ***before*** publication
- What is needed is a way that allows the TO to publish (the hash of) the keys without knowing which hands will come out
- This can be done by adding some information

- This information must be unknowable to the TO at publication time
- And it must be public knowledge before the start of the tournament
- My suggestion is the closing Dow Jones Index some day between publication and tournament

Second attempt (2)

- So just as first attempt, TO publishes (the hash of) the keys, and also which delayed information he will use
- The hands are generated by seeding BigDeal with hash(key, delayed information)
- The TO cannot know this in advance, so the hands are unknown to him at publication time
- After the tournament the TO publishes the keys, the public has them now and has the delayed information(from newspaper/website)
- The public can check hands

Demo

- Working title of current software is “SquareDeal”

- Two computers, one is TO, one is public
- Publication for the demo is done by memory-stick
- In real life by Email and/or tournament-website

Summary

- Potential problem: distrust of competitors to organizer
- Problem solved with same technology as BigDeal already uses
- Further details to be discussed if interested

- Thank you for your attention